Université Paul Sabatier - UFR MIG - Département de Mathématique.
Année scolaire 2010/2011.

Cours polycopié pour le module Mathématique II

Conventions. Nous noterons $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{R}$ l'ensemble des nombres réels, $\mathbb{C}$ l'ensemble des nombres complexes. Toutes ces notions (y compris la notion d'ensemble) seront détaillées plus bas.

Dans ce qui suit, les *mots en italiques* sont ceux que l'on est en train de définir. On emploie le symbole := lorsqu'une égalité sert à définir le membre gauche à partir du membre droit. Par exemple : On appelle *carré* du réel x le réel $x^2 := x.x$. On peut aussi introduire un terme sans définition complète et sans que sa connaissance soit exigible : on le mettra plutôt entre guillemets. Par exemple : On résume les propriétés de l'addition dans $\mathbb{R}$ en disant que $(\mathbb{R}, +)$ est un "groupe commutatif".

À propos du module Math II (UE8). Tous les étudiants qui suivent le module Math II suivent par ailleurs le module Math I (UE2), qui vise essentiellement à consolider les acquis du secondaire afin de servir aux sciences exactes, comme à la suite de l'enseignement mathématique. *A contrario*, on adopte ici un style propre aux mathématiciens : mise en avant des fondements (axiomes et définitions), des concepts abstraits, des démonstrations.

Ce cours à destination des étudiants de l'UE de Mathématique II est assez détaillé et contient des compléments qui vont parfois au delà du programme prévu. Comme tout cours de Mathématique, il doit être lu avec un stylo et une feuille de papier blanche à la main pour vérifier pas à pas que toutes les assertions sont correctes. Chaque section de ce cours se termine par des exercices non corrigés à "consommer sans modération". Il est vivement conseillé de s'exercer à résoudre par soi-même ces exercices sans avoir une solution à coté : c'est grâce à ce travail personnel indispensable que l'on peut aller plus loin dans la compréhension et l'assimilation des notions mathématiques introduites. C'est la seule méthode connue à ce jour pour progresser en mathématiques. Certains de ces exercices seront corrigés pendant les séances de TD, mais pas tous, faute de temps. N'hésitez pas à demander de l'aide aux enseignants si un exercice vous résiste !

Les exercices sont classés en trois catégories :

- Ceux dont le numéro n'est pas suivi d'étoile sont élémentaires. Ils permettent de se familiariser avec les notions introduites en cours. On doit pouvoir les faire sans presque réfléchir.
- Les exercices (*) demandent un petit peu de réflexion, mais restent cependant tout à fait faciles à faire une fois que l'on a assimilé les techniques standard pour les résoudre.
- Les exercices (**) sont eux plus difficiles : ils demandent d'avoir bien compris les notions, ils sont parfois plus longs et certaines questions peuvent être dures. Il ne faut pas hésiter à y consacrer parfois plusieurs heures : c'est en essayant de résoudre ces exercices que l'on progressera en mathématiques.

Enfin, certaines parties du texte sont en petits caractères, comme cela. Elles ne sont pas essentielles pour la suite et l'on peut les sauter en première lecture. Cependant, les étudiants curieux auront avantage à les lire, quitte à ne pas tout comprendre. Elles donnent souvent un éclairage différent sur certains points du cours, ou introduisent des notions qu'on retrouvera plus tard dans d'autres cours de mathématiques.

Références et compléments. Il existe plusieurs ouvrages que l'on peut consulter et qui se trouvent à la Bibliothèque Universitaire. Citons entre autres :

- *Les mathématiques en Licence, Tome 1* par Élie Azoulay, Jean Avignant et Guy Auliac. Éditions ÉdiScience. Ce livre est très abordable.
- *Mathématiques. Tout-en-un pour la Licence. Niveau L1* sous la direction de Jean-Pierre Ramis et André Warusfel, Éditions Dunod. Ce livre est particulièrement conseillé pour les nombreux compléments, éclaircissements et exercices supplémentaires qu'il contient.
- *Cours de Mathématiques du premier cycle*, par Jacques Dixmier, Éditions Gauthier-Villars.
- *Mathématiques pour le DEUG, Analyse Première année*, par François Liret et Dominique Martinais, Éditions Dunod.

Site web Vous trouverez une version électronique du polycopié, mais aussi les sujets de devoirs et d'examens donnés l'an passé, sur la page web :

`http://www.math.univ-toulouse.fr/~barthe/L1math2/`

Chapitre 1

Éléments de Logique et de théorie des ensembles

1.1 Logique

La logique est le langage des mathématiques. C'est une discipline à part entière, dont nous ne présentons ici que les bases élémentaires, qui permettront aux lecteurs de se familiariser avec les raisonnements mathématiques.

1.1.1 Énoncés

Un *énoncé* est une phrase ayant un sens mathématique précis, et qui peut être soit vrai, soit faux (mais jamais "entre les deux", ou "ni l'un ni l'autre"). Nous n'entrons pas dans la discussion de savoir quels types d'énoncés peuvent être considérés comme "mathématiques". Mais le lecteur verra au fur et à mesure des exemples ce que peut signifier un énoncé (ou une proposition).

Exemple d'énoncé : "$2 > 3$" (c'est un énoncé faux).

Un énoncé peut dépendre d'une variable. Par exemple $P(x)$: "$x > 3$". Alors $P(2)$ est faux mais $P(4)$ est vrai.

Il peut aussi dépendre de plusieurs variables. $P(x, y)$: "$x + y = 2$". Alors $P(1, 1)$ est vrai, mais $P(2, 1)$ est faux.

Quand on a un énoncé P, on a l'énoncé contraire, sa *négation*, $(nonP)$ encore noté $\bar{P}$ qui est vrai lorsque P est faux et faux lorsque P est vrai.

Ainsi, si $P(x)$: "$x > 3$, $(nonP)(x)$: "$x \leq 3$" (et non pas $x < 3$! !).

La négation de la négation d'un énoncé est l'énoncé de départ.

$$non(nonP) = P.$$

1.1.2 Quantificateurs

Il y en a deux. Ce sont les deux symboles $\forall$ (Quel que soit) et $\exists$ (Il existe).

Le symbole $\forall$ vient de l'allemand Alle, et $\exists$ de Existieren.

$\forall x \in E, P(x)$ se lit "Pour tout x dans l'ensemble E, $P(x)$ est vraie". C'est un nouvel énoncé fabriqué à partir de l'énoncé P. Nous n'avons pas encore vu ce qu'est un ensemble, ni ce que veut dire "x est dans l'ensemble E", mais nous espérons que la signification de cette phrase est bien claire pour tout le monde.

Par exemple, avec $P(x) : x > 3$, on voit que "$\forall x > 4, P(x)$" est un énoncé vrai, tandis que "$\forall x > 2, P(x)$" est un énoncé faux.

"$\exists x \in E, P(x)$" se lit "Il existe un élément x de l'ensemble E pour lequel $P(x)$ est vrai". On l'écrit aussi parfois "$\exists x \in E \mid P(x)$"

Ainsi, toujours avec $P(x) : x > 3$, "$\exists x > 2 \mid P(x)$" est vrai tandis que "$\exists x < 2 \mid P(x)$" est faux.

Dans ces deux derniers exemples, l'ensemble E est l'ensemble des nombres supérieurs strictement à 2 dans le premier cas, et strictement inférieurs à 2 dans le second. Ici, il faut faire attention : l'ensemble de nombres dont on parle peut être l'ensemble des entiers naturels, ou bien celui des nombres rationnels, ou celui des nombres réels, ou tout autre ensemble de nombres. Normalement, il faudrait l'indiquer dans l'énoncé, mais on suppose implicitement que cet ensemble de nombres est clair d'après le contexte : si l'on fait de l'arithmétique, ce sera l'ensemble des entiers, si on fait de l'analyse (des suites..) ce sera l'ensemble des nombres réels, etc... En tout cas, on suppose toujours dans un énoncé que l'ensemble E dont on parle est bien défini sans ambiguïté.

Avec ces quantificateurs, on peut donc construire de nouveaux énoncés, qui peuvent devenir de plus en plus compliqués. Ainsi,

"$\exists y > 2, \forall x > y, P(x)$", ou bien encore

$$Q(z) : \forall y > z, \exists x < y \mid P(x).$$

Une fois mise dans un quantificateur, une variable devient "muette" : c'est un nom arbitraire que nous lui avons donné. On peut changer son nom en un autre, **à condition de ne pas lui donner le nom d'une autre variable apparaissant ailleurs dans l'énoncé**.

Il faut bien comprendre l'usage de cette lettre "muette" dans un énoncé. Rien ne nous oblige à l'appeler par une lettre : on aurait aussi bien pu l'appeler "Untel" : l'important est qu'il ne désigne personne en particulier : on n'aurait pas pu l'appeler "2", par exemple, car "2" fait référence à un nombre bien défini.

Par exemple, "$\forall x \in E, P(x)$" et "$\forall a \in E, P(a)$", sont les mêmes énoncés.

Mais "$\exists y > 2 \mid \forall x \geq y, P(x)$" n'est pas la même chose que "$\exists x > 2 \mid \forall x \geq x, P(x)$".

La règle de **négation des propositions avec quantificateurs** est

$$non"\forall x \in E, P(x)" = "\exists x \in E, nonP(x)",$$

et

$$non"\exists x \in E, P(x)" = "\forall x \in E, nonP(x)".$$

Attention, une erreur fréquente (surtout dans les énoncés compliqués comme ceux qui apparaîtrons à la fin de ce cours) est de penser que la négation de "$\forall x \in E, P(x)$" est $\exists x \in E^c \mid P(x)$, où E^c est le complémentaire de E (voir prochaine section).

Ainsi, la négation de la proposition (fausse) "$\forall x > 2, x > 3$" est "$\exists x > 2 \mid x \leq 3$" et non pas "$\exists x \leq 2 \mid x \leq 3$".

Exercice 1. Quelle est la négation de l'énoncé $\exists x > a, \forall y < x, y > 4$?

On ne peut pas intervertir deux quantificateurs $\forall$ et $\exists$ successifs.

Ainsi, "$\forall x \in E,\ \exists y \in F,\ P(x, y)$" n'est pas la même chose que "$\exists y \in F, \forall x \in E, P(x, y)$" (mais est la même chose que "$\forall y \in E, \exists x \in F, P(y, x)$", en vertu de la règle de changement de nom).

Par exemple, "$\forall x > 3,\ \exists y > 2,\ y > x$" est vrai, mais "$\exists y > 2,\ \forall x > 3,\ y > x$" est faux.

Par contre, on peut intervertir "$\forall x \in E,\ \forall y \in F, P(x,y,z)$" et "$\forall y \in F, \forall x \in E, P(x,y,z)$" et de même "$\exists x \in E,\ \exists y \in F,$" et "$\exists y \in F, \exists x \in E,$". C'est-à-dire deux quantificateurs **successifs et de même type**.

Il faut faire attention ici à ce que les quantificateurs soient bien successifs. Ainsi, "$\forall x \in E, \exists y \in F,\ \forall z \in G,\ P(x,y,z)$" n'est pas la même chose que "$\forall z \in G, \exists y \in F,\ \forall x \in E,\ P(x,y,z)$".

Ainsi, par exemple, pour x, y, z dans l'ensemble à deux éléments $\{1,2\}$, la proposition

$$\forall x, \exists y, \forall z, x = y \text{ et } y \leq z+1$$

est vraie, alors que

$$\forall z, \exists y, \forall x, x = y \text{ et } y \leq z+1$$

est fausse. Ce qui est caché ici, c'est qu'on a intervertit un "quelque soit" et un "il existe". Une autre situation où l'on peut intervertir $\forall$ et $\exists$ est la suivante. Si $\exists y, \forall x, P(x,y)$ est vrai, alors $\forall x, \exists y, P(x,y)$ est aussi vraie. Mais le contraire est faux (**et source d'un très grand nombre d'erreurs**).

1.1.3 Connecteurs logiques

Conjonction et disjonction

Ils servent à créer de nouveaux énoncés à partir de plusieurs. Ils se notent $\vee$ ("ou") et $\wedge$ ("et"). Nous en avons vu déjà des exemples plus haut. Ainsi

$P \vee Q$ (lire "P ou Q") est vrai si et seulement si P est vrai ou Q est vrai.

Attention, cela n'exclut pas que les deux énoncés puissent être vrais en même temps ! Ce n'est pas un ou "exclusif" comme dans "fromage ou dessert".

$P \wedge Q$ (lire "P et Q") est vrai si et seulement si à la fois P est vrai et Q est vrai.

Par exemple, avec $P(x)$: "$x > 2$" et $Q(y)$: "$y < 3$", $(P \vee Q)(x)$ est toujours vrai, tandis que $(P \wedge Q)(x)$ n'est vrai que si $2 < x < 3$.

Ils s'échangent l'un et l'autre par la négation.

$$non(P \wedge Q) = (nonP) \vee (nonQ),\ non(P \vee Q) = (nonP) \wedge (nonQ).$$

Les opérations $\vee$ et $\wedge$ sont "commutatives", c'est à dire

$$P \wedge Q = Q \wedge P,\ P \vee Q = Q \vee P.$$

Les opérations $\vee$ et $\wedge$ sont "associatives", c'est à dire

$$(P \wedge Q) \wedge R = P \wedge (Q \wedge R),\ (P \vee Q) \vee R = P \vee (Q \vee R).$$

C'est pourquoi on les note sans risquer d'erreur $P \wedge Q \wedge R$ et $P \vee Q \vee R$.

Les opérations $\vee$ et $\wedge$ sont "distributives l'une par rapport à l'autre", c'est-à-dire

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R),\ P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R).$$

Enfin, quel que soit l'énoncé P, $P \wedge (nonP)$ est faux tandis que $P \vee (nonP)$ est vrai.

L'implication

C'est un énoncé de la forme "si P est vrai, alors Q l'est aussi". On le note $P \Longrightarrow Q$. Sur le plan formel, ce n'est rien d'autre que $(nonP) \vee Q$. En d'autres termes, soit P est faux, soit P est vrai et Q est aussi vrai.

Ici, il y a un souci. Formellement, d'après ce qu'on vient de dire, P et Q peuvent dépendre d'un paramètre. Ainsi $(x > 2) \Longrightarrow (x \leq 3)$ est vrai pour $x \leq 3$ et faux pour $x > 3$, ce qui n'est bien sûr pas ce que l'on entend par là.

Lorsque P et Q dépendent du même paramètre x, alors on dit que $P \Longrightarrow Q$ lorsque

$$\forall x,\ P(x) \Longrightarrow Q(x).$$

La *réciproque* de l'implication $P \Longrightarrow Q$ est l'implication $Q \Longrightarrow P$.

Deux énoncés sont *équivalents* (on note $P \iff Q$) si on a à la fois $P \Longrightarrow Q$ et $Q \Longrightarrow P$.

La *contraposée* de l'implication "$P \Longrightarrow Q$" est l'implication "$nonQ \Longrightarrow nonP$".

En fait

$$(nonQ \Longrightarrow nonP) \iff (P \Longrightarrow Q).$$

En effet,

$$(nonQ \Longrightarrow nonP) = (non(nonQ) \vee nonP) = (Q \vee nonP) = (P \Longrightarrow Q).$$

Attention, il ne faut pas confondre réciproque et contraposée.

La contraposée est une "autre manière de dire la même chose", tandis que la réciproque est un énoncé différent de l'énoncé de départ. La contraposée est à la base du raisonnement par l'absurde.

L'implication est "transitive" Si $P \Longrightarrow Q$ et $Q \Longrightarrow R$ sont vraies, alors $P \Longrightarrow R$ est vraie.

Cette transitivité peut se propager à plusieurs énoncés. Ainsi

$$P_1 \Longrightarrow P_2 \Longrightarrow P_3 \Longrightarrow \ldots \Longrightarrow P_n.$$

On peut ainsi obtenir des équivalences grâce au "**théorème tournant**". Pour démontrer des équivalences entre énoncés, il suffit de montrer des implications en boucle.

Si

$$P_1 \Longrightarrow P_2 \Longrightarrow P_3 \Longrightarrow \ldots \Longrightarrow P_n \Longrightarrow P_1,$$

alors

$$P_1 \iff P_2 \iff P_3 \iff \ldots \iff P_n.$$

L'unicité

On dit qu'un élément x dans un ensemble E ayant la propriété P est unique si deux éléments de E pour lesquels $P(x)$ est vraie sont nécessairement égaux. Ceci se traduit par

$$\forall x \in E, \forall y \in E,\ P(x) \wedge P(y) \Longrightarrow x = y.$$

Ainsi, si $P(x) = (x \leq 2) \wedge (x \geq 2)$ alors x est unique.

Attention, l'unicité n'implique pas l'existence. Ainsi, un x qui vérifie $(x > 2) \wedge (x < 2)$ est unique (mais il n'existe pas !).

Lorsqu'il y a existence et unicité, on utilise souvent le symbole $\exists !$.

Ainsi $\exists ! x, (x \leq 2) \wedge (x \geq 2)$ (cet unique x est bien sûr $x = 2$).

1.1.4 Différents types de raisonnement

Le raisonnement direct ou syllogisme

Si $A \Longrightarrow B$ et que A est vrai, alors B est vrai. On l'utilise pour montrer que B est vrai.

Par exemple si l'on veut démontrer que $x > 3 \Longrightarrow x > 2$, on écrit que, si $x > 3$, puisque $3 > 2$ et que la relation $a > b$ et transitive, alors $x > 2$.

Le raisonnement par contraposée

Si A est vrai et que $nonB \Longrightarrow nonA$, alors B est vrai. "Si B était faux, alors A serait faux aussi, or A est vrai, et donc B l'est.

Reprenons l'exemple précédent en le compliquant un peu : montrons (dans l'ensemble $\mathbb{N}$) que

$$\{x > a \Longrightarrow x > b\} \Longrightarrow a \geq b.$$

Ici $P = \{x > a \Longrightarrow x > b\}$ et $Q = \{a \geq b\}$. Supposons $nonQ$, qui est $b > a$. Si l'on choisit alors $x = b$, alors pour cet x là, on a $x > a$ et $non"x > b$: donc l'implication $\{x > a \Longrightarrow x > b\}$ est fausse et on a $nonP$. Donc $nonQ \Longrightarrow nonP$ et par conséquent $P \Longrightarrow Q$.

Le raisonnement par l'absurde

Si A est vrai et que $A \wedge (nonB)$ est faux, alors B est vrai. Dans la pratique, il est très proche du raisonnement par contraposée.

Le raisonnement par disjonction des cas

Si l'on sait que A est équivalent à $A_1 \vee A_2 \ldots \vee A_n$, et que $A_1 \Longrightarrow B$, $A_2 \Longrightarrow B$, $\ldots A_n \Longrightarrow B$, alors $A \Longrightarrow B$.

Par exemple pour montrer que $x > 0 \Longrightarrow x^2 + \frac{1}{x} \geq 1$, il est commode de distinguer deux cas. Si $x \geq 1$ alors $x^2 \geq 1$ et on a bien $x^2 + \frac{1}{x} \geq 1$. Si $x \in (0, 1]$ alors $1/x \geq 1$ et donc $x^2 + \frac{1}{x} \geq 1$.

Le raisonnement par récurrence

Il s'agit d'une propriété $P(n)$ qui dépend d'un nombre entier n et qu'on veut démontrer pour tout $n \geq n_0$ (dans la pratique n_0 vaut souvent 0 ou 1).

On commence par démontrer $P(n_0)$ (c'est l'initialisation), et ensuite on montre que pour tout $n \geq n_0$, $P(n) \Longrightarrow P(n+1)$ (on dit que P est héréditaire). Alors $P(n)$ sera vraie pour tous les entiers n à partir de n_0. Ce principe de démonstration est appelé récurrence simple. Nous y reviendrons au chapitre suivant et nous présenterons des variantes utiles.

1.2 Ensembles

Le vocabulaire et les notations de la théorie des ensembles sont centraux dans toutes les mathématiques. La théorie des ensembles "naïve" que nous décrivons ici laisse dans l'ombre pas mal de difficultés sérieuses (par exemple, on ne dit jamais explicitement ce qu'est un ensemble). Ce n'est pas par paresse, mais parce qu'une étude approfondie de ces notions nous entraînerait trop loin. Ce qui est important, ce sont les relations entre ensembles et éléments, ce qu'on a le droit de faire et ce qui est illicite, etc. Ce que nous présentons ici, c'est le vocabulaire et les principes de base qui seront utiles non seulement tout au long de ce cours, mais tout au long de vos études en mathématiques.

Comme nous l'avons déjà dit, nous n'allons pas définir ce qu'est un *ensemble*. C'est intuitivement une "collection d'objets". On doit imaginer ces objets comme non rangés, sans répétitions possibles. Les objets n'ont pas besoin d'appartenir à une classe d'objets mathématiques précise. Ainsi, $\{1, 2, 3, \text{noir}, \text{blanc}, \text{Paul}, \text{Marie}\}$ est un ensemble. Au sens strict, $\{1, 1, 2\}$ n'en est pas un puisque l'élément 1 est répété. Cependant, par convention, on considèrera que c'est une notation maladroite pour l'ensemble $\{1, 2\}$.

Les ensembles peuvent être finis (c'est à dire qu'ils n'ont qu'un nombre fini d'éléments, comme l'ensemble qui précède), ou bien infinis, comme l'ensemble des entiers naturels, des nombres réels, des nombres complexes, des droites du plan, etc...

Nous allons définir des relations entre objets et ensembles, ainsi que beaucoup de vocabulaire un peu abstrait. On verra bientôt que n'importe quoi ne peut pas être un ensemble.

1.2.1 Définitions

Nous ne définissons pas non plus ce que veut dire le verbe *appartenir*. On dit que a "appartient" à l'ensemble A (et on note $a \in A$) si a est l'un des objets de la collection A. On dit encore que a est un *élément* de A.

On notera $a \notin A$ si a n'appartient pas à A. Nous ne définissons pas ce que veut dire le signe "=". Intuitivement, $a = b$ veut dire que ce sont les mêmes objets (ces objets peuvent eux-même être des ensembles). S'ils sont différents, on note $a \neq b$. Si $a = b$ et $b = c$, alors $a = c$.

Une propriété fondamentale qui permet d'identifier un ensemble est qu'il est entièrement caractérisé par les objets qu'il contient.

Deux ensembles sont égaux s'ils ont les mêmes éléments.

Plus exactement, en langage mathématique,

$$A = B \iff \{(x \in A) \iff (x \in B)\}.$$

Cette propriété (intuitivement évidente) est fondamentale dans la pratique. Pour montrer que deux ensembles A et B sont égaux, on montre que tout élément de A est un élément de B, et réciproquement. Les propriétés de l'égalité s'appliquent bien évidement aux ensembles.

L'ensemble vide, noté $\emptyset$, est un ensemble qui n'a aucun élément. D'après la propriété précédente, il est unique. C'est l'ensemble tel que

$$\forall x, x \notin \emptyset.$$

On n'est pas obligé de voir directement qu'un ensemble défini par une certaine propriété est vide. C'est l'impossiblité pour n'importe quel x d'être dans cet ensemble qui fait de cet ensemble l'ensemble vide. Par exemple, l'ensemble des nombres réels tels que $x^2 = -1$ est l'ensemble vide. (Mais il n'est pas vide si on considère des nombres complexes, bien qu'on puisse décrire l'ensemble pas la même formule).

Lorsqu'un ensemble E n'a qu'un nombre fini d'éléments, on appelle ce nombre d'éléments le *cardinal* de l'ensemble, on le notera card E ou parfois $\sharp E$. Ainsi card $\emptyset = 0$, card $\{Blanc, noir\} = 2$. Compter le nombre d'éléments d'un ensemble fini peut être une tâche assez compliquée (surtout quand cet ensemble dépend d'un paramètre $n \in \mathbb{N}$). C'est l'objet du chapitre "dénombrement" ou de "l'analyse combinatoire".

Pour définir un ensemble, on dispose de plusieurs méthodes.

Tout d'abord, si on connait tous les éléments $a_1, \ldots, a_n$ de l'ensemble A, on notera $A = \{a_1, \ldots, a_n\}$. On dit alors que l'ensemble est défini en *extension*. Rappelons que l'ordre n'a pas

d'importance et ainsi que $\{1,2,3\}$ et $\{3,2,1\}$ désignent le même ensemble. (On verra plus bas comment tenir compte de l'ordre, quand on parlera de dénombrement).

Il faut faire attention ici aux répétitions. Ainsi, $\{2,2,2\}$ désigne en fait l'ensemble dont le seul élément est 2, c'est à dire $\{2\}$. Son cardinal est 1.

De même

$$\{1,2,3,2,4,2\} = \{1,2,3,4\}.$$

Comme on le voit, il y a plein de façons différentes d'écrire un ensemble en *extension*.

Cette possibilité de répéter plusieurs fois le même élément est parfois indispensable. Par exemple, dans l'énoncé suivant Pour tous les réels a, b, c tels que $b^2 \geq 4ac$ et $a \neq 0$, l'ensemble des solutions de l'équation $ax^2 + bx + c = 0$ est

$$\left\{ \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \frac{-b - \sqrt{b^2 - 4ac}}{2a} \right\}$$

est un énoncé vrai, même lorsque $b^2 = 4ac$, auquel cas cet ensemble n'a plus qu'un seul élément, et non pas deux comme il paraît au premier abord.

On peut aussi définir un ensemble par une propriété mathématique. Ainsi, l'ensemble des entiers multiples de 3, ou bien l'ensemble des nombres réels x tels que $2 < x < 3$.

Nous n'avons pas vraiment défini ce qu'est une propriété mathématique. Mais il y a des définitions illicites qui ne peuvent pas donner des ensembles. Ainsi, "l'ensemble des nombres entiers qu'on ne peut pas définir en moins de 100 mots dans la langue française" : ce n'est en fait pas un ensemble (l'idée est que cette définition est bien trop vague). Pour toucher du doigt les difficultés qu'on a à définir proprement des ensembles, acceptons cette propriété de l'ensemble $\mathbb{N}$ des entiers naturels : *tout sous ensemble de* $\mathbb{N}$ *non vide possède un plus petit élément.* Tout le monde conviendra que cette propriété est tout à fait légitime.

Alors, si l'ensemble des nombres entiers qu'on ne peut pas définir en moins de 100 mots dans la langue française était vraiment un ensemble, (on se convainc sans mal qu'il n'est pas vide, car avec moins de 100 mots, on ne peut définir qu'un nombre fini d'entiers, et il y a un nombre infini d'éléments de $\mathbb{N}$). Son plus petit élément serait "le plus petit entier qu'on ne peut pas définir en moins de 100 mots de la langue française", mais cette définition comprend moins de 100 mots, et donc cet entier n'appartient pas à l'ensemble dont il est le plus petit élément, ce qui est en contradiction avec la propriété des sous-ensembles non vides de $\mathbb{N}$ que nous avons acceptée plus haut.

Comme quoi, on ne peut pas faire n'importe quoi avec les ensembles. Mais nous éviterons bien d'entrer dans ce genre de considérations, et tous les ensembles que nous rencontrerons seront proprement définis.

On peut fabriquer des ensembles dont les éléments sont eux-mêmes des ensembles (on le fera très souvent). Ainsi, si $A = \{1,2\}$ et $B = \{2,3\}$, on a l'ensemble $\{A, B\} = \{\{1,2\},\{2,3\}\}$ qui a deux éléments, qu'il ne faut pas confondre avec $\{1,2,2,3\} = \{1,2,3\}$ qui en a trois. De même, l'ensemble $\{\{1,2,3\}\}$ n'a qu'un seul élément.

Exercice 2. Combien l'ensemble $\{\{\{1,2\},\{2,3\}\}\}$ a-t-il d'éléments ?

Sous-ensembles

On dit qu'un ensemble A est *inclus* dans un ensemble B (et on note $A \subset B$) si tous les éléments de A sont des éléments de B, en d'autres termes

$$A \subset B \iff \Big((x \in A) \Longrightarrow (x \in B) \Big).$$

On note parfois $A \subsetneq B$ pour indiquer que A est inclus dans B mais ne lui est pas égal.
On a toujours $\emptyset \subset A$, et

$$\Big((A \subset B) \wedge (B \subset C)\Big) \Longrightarrow A \subset C.$$

Si $x \in A$, on peut lui faire correspondre un sous ensemble $\{x\}$, qui est le sous-ensemble qui contient x et lui seul : c'est un *singleton*. Il ne faut pas le confondre avec l'élément x : x est un élément de A, $\{x\}$ est un sous-ensemble de A.

De même, lorsqu'on a deux éléments x et y de A, on peut lui faire correspondre le sous-ensemble $\{x, y\}$, qui est une paire (et un singleton si $x = y$!). On peut de même considérer des triplets, des quadruplets, etc.

La *réunion* de A et B est l'ensemble $A \cup B$ dont les éléments sont ceux de A et ceux de B. En d'autres termes, x appartient à $A \cup B$ si et seulement si x appartient à A **ou** x appartient à B.

$$\Big(x \in A \cup B\Big) \iff \Big((x \in A) \vee (x \in B)\Big).$$

L'*intersection* de A et B est l'ensemble $A \cap B$ dont les éléments sont formés de ceux qui appartiennent à la fois à A et à B. En d'autres termes, x appartient à $A \cap B$ si et seulement si x appartient à A **et** x appartient à B.

$$\Big(x \in A \cap B\Big) \iff \Big((x \in A) \wedge (x \in B)\Big).$$

Les éléments de B qui ne sont pas dans A forment la *différence* $B \setminus A$.

Lorsque $A \subset B$, on dit que A est un sous ensemble de B. L'ensemble formé des éléments de B qui ne sont pas dans A s'appelle le complémentaire de A dans B. C'est encore $B \setminus A$. Souvent, l'ensemble B est sous-entendu (pas exemple l'ensembles des entiers naturels, ou des nombres réels, ou bien des droites du plan, etc..) et on oublie B alors dans la notation. On note A^c pour le complémentaire de A.

Attention, la notation A^c suppose qu'on a un ensemble E de référence dans lequel on a le complémentaire.

Ainsi, le complémentaire de $\{1, 2\}$ n'est pas le même si l'ensemble de référence est $\{1, 2, 3\}$, auquel cas c'est $\{3\}$, ou bien l'ensemble des entiers naturels $\mathbb{N}$, auquel cas le complémentaire est $\{0\} \cup \{n, n \geq 3\}$.

Ainsi, lorsqu'on a un ensemble de référence E, et deux sous-ensembles A et B de E, alors $B \setminus A = B \cap A^c$.

Dans la pratique, l'ensemble de référence E sera toujours bien déterminé, et il n'y aura aucune ambiguïté quand on parlera de A^c.

Les règles de calcul sur les ensembles sont calquées sur celles de la logique, ou le passage au complémentaire remplace la négation, l'union remplace $\vee$ et l'intersection remplace $\wedge$, l'inclusion remplace l'implication.

Ainsi,

$$(A^c)^c = A,\ (A \cup B)^c = A^c \cap B^c,\ (A \cap B)^c = A^c \cup B^c,$$
$$A \cup B = B \cup A,\ A \cap B = B \cap A,$$
$$A \cup (B \cup C) = (A \cup B) \cup C,\ (A \cap B) \cap C = A \cap (B \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
$$A \subset B \iff B^c \subset A^c.$$

Exercice 3. Démontrer les trois premières égalités (en revenant à la définition : deux ensembles sont égaux signifie que tout élément de l'un est un élément de l'autre et réciproquement).

Ensemble des parties d'un ensemble

Lorsqu'on a un ensemble A, on peut considérer tous ses sous-ensembles, qu'on appelle parties de A. Ces parties forment elles-mêmes un ensemble, qu'on appelle *l'ensemble des parties de* A, et qu'on note $\mathcal{P}(A)$. On retiendra donc que

$$X \in \mathcal{P}(A) \iff X \subset A.$$

Ainsi, si $A = \{1, 2\}$,

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

L'ensemble vide est toujours un sous-ensemble de n'importe quel ensemble.

Ceci s'applique bien sûr aussi à l'ensemble vide (attention, ici, on va commencer à se prendre un peu la tête, mais les considérations qui suivent sont toutes sauf gratuites). On a aussi $\mathcal{P}(\emptyset) = \{\emptyset\}$, qu'il ne faut pas confondre avec $\emptyset$. Ainsi, $\{\emptyset\}$ est un ensemble (qui a un élément, qui est $\emptyset$) et donc il n'est pas vide, et de même $\{\{\emptyset\}\}$, ou même $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ qui a deux éléments.

Puisque $\mathcal{P}(A)$ est un nouvel ensemble, on peut encore considérer $\mathcal{P}(\mathcal{P}(A))$, et puis encore $\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$ et ainsi de suite. On a aussi $A \cup \mathcal{P}(A)$ ainsi que $\mathcal{P}(A \cup \mathcal{P}(A))$, etc. Comme on le voit, dès qu'on a un ensemble, on en obtient beaucoup d'autres.

Nous verrons dans le chapitre dénombrement que si A est un ensemble fini a n éléments, alors $\mathcal{P}(A)$ a 2^n éléments.

Nous avons bien évidement

$$A \subset B \Longrightarrow \mathcal{P}(A) \subset \mathcal{P}(B).$$

Exercice 4. Démontrez-le à partir des définitions !

Couples et produits d'ensembles

Une autre façon de construire des ensembles est de considérer des *couples*. Lorsqu'on dispose de deux ensembles A et B, on peut considérer l'ensembles des ou couples (a, b) avec $a \in A$ et $b \in B$. L'ensemble de ces couples constitue l'ensemble *produit* $A \times B$.

Rien n'interdit de choisir $A = B$, mais **attention** : $A \times A$ n'est pas l'ensemble des couples (a, a) qui est par définition la *diagonale* de $A \times A$.

Ainsi, si $A = \{1, 2\}$, $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$. Contrairement aux points d'un ensemble, il faut faire attention à l'ordre ici : $(1, 2) \neq (2, 1)$.

Si A a n éléments et B a m éléments, alors $A \times B$ possède $n.m$ éléments. On pourra le démontrer par exemple par récurrence sur m.

Relations

Une *relation* sur un ensemble A est une partie $\mathcal{R}$ de $A \times A$: les couples (a, b) qui sont dans $\mathcal{R}$ sont dits en relation, et on note $a\mathcal{R}b$ au lieu de $(a, b) \in \mathcal{R}$.

Un exemple de relation est $x \leq y$ sur $\mathbb{N} \times \mathbb{N}$. On fait parfois la distinction entre la relation $a\mathcal{R}b$ et la partie de $A \times B$ qui la définit, qu'on appelle le *graphe* de la relation, car il n'est souvent pas commode de penser une relation comme un ensemble (encore moins un ensemble dans un produit !).

On peut tout aussi bien définir des relations entre $a \in A$ et $b \in B$ comme une partie $\mathcal{R}$ de $A \times B$. Nous ne le ferons pas car nous n'en aurons pas besoin.

Les relations peuvent bénéficier de plusieurs propriétés. Nous en donnons une liste (un peu longue, mais autant se familiariser dès maintenant avec le vocabulaire).

(1) Une relation $\mathcal{R}$ sur A est dite *réflexive* si, $\forall a \in A,\ a\mathcal{R}a$.

(2) Une relation $\mathcal{R}$ sur A est dite *symétrique* si, $a\mathcal{R}b \Longrightarrow b\mathcal{R}a$.

(3) Une relation $\mathcal{R}$ sur A est dite *antisymétrique* si, $\Big((a\mathcal{R}b) \wedge (b\mathcal{R}a)\Big) \Longrightarrow a = b$.

(4) Une relation $\mathcal{R}$ sur A est dite *transitive* si, $\Big((a\mathcal{R}b) \wedge (b\mathcal{R}c)\Big) \Longrightarrow a\mathcal{R}c$.

(5) Une relation qui est à la fois, réflexive, symétrique et transitive est une *relation d'équivalence*. (Par exemple, sur l'ensemble des entiers relatifs, "$x - y$ est pair" est une relation d'équivalence).

(6) Une relation qui est à la fois réflexive, antisymétrique et transitive est une *relation d'ordre*. (Par exemple, "$x \leq y$" sur $\mathbb{R}$ est une relation d'ordre.)

Exercice 5. Est-ce que la relation "$x < y$" sur $\mathbb{R}$ est une relation d'ordre ?

Lorsqu'on a une relation d'équivalence (souvent notée $a \sim b$), on peut considérer un nouvel ensemble, *l'ensemble quotient*. C'est une notion importante, que l'on reverra souvent dans différents contextes.

Tout d'abord, si on considère $a \in A$, on peut regarder l'ensemble des $b \in A$ tels que $a \sim b$. C'est un ensemble non vide, et on le note $\dot{a}$: c'est la *classe d'équivalence de* a. On remarque que $a \in \dot{a}$, et que si $a \neq b$, ou bien $\dot{a} = \dot{b}$, ou bien $\dot{a} \cap \dot{b} = \emptyset$ (Pourquoi ?).

L'ensemble des $\dot{a}, a \in A$ forme donc une famille $\mathcal{Q}$ de sous ensembles de A qui a les trois propriétés suivantes

(i) Aucun des éléments de $\mathcal{Q}$ n'est vide

(ii) Tout point de A appartient à l'un des éléments de $\mathcal{Q}$.

(iii) L'intersection de deux éléments différents de $\mathcal{Q}$ est toujours vide

Lorsqu'on a famille $\mathcal{Q}$ de sous-ensembles de A qui vérifient ces trois propriétés, on dit qu'on a une *partition* de A.

L'ensemble $\{\dot{a}, a \in A\}$ (qui est un sous ensemble de $\mathcal{P}(A)$, donc un élément de $\mathcal{P}(\mathcal{P}(A))$!) est appelé l'ensemble quotient de A par la relation $\sim$. On le note souvent $A/\sim$. L'opération de passage au quotient revient à ne plus distinguer deux éléments de E qui sont dans la même classe d'équivalence.

Ainsi, si on considère sur l'ensemble $\mathbb{N} \times \mathbb{N}^*$ ($\mathbb{N}^* = \mathbb{N} \setminus \{0\}$) la relation

$$(n, p) \sim (n', p') \iff np' = n'p,$$

on vérifie que c'est une relation d'équivalence (exercice !) et l'ensemble quotient n'est rien d'autre que l'ensemble des nombres rationnels positifs ou nuls.

Remarquons que si on se donne une partition de A, on peut fabriquer une relation d'équivalence en décidant que deux points sont en relation si et seulement si ils sont dans le même sous ensemble de la partition. Il y a donc une analogie étroite entre relations d'équivalence et partitions (c'est même formellement plus ou moins la même chose).

Exercice 6. Démontrer l'assertion qui précède.

Unions et intersections quelconques

Nous avons vu plus haut que $(A \cup B) \cup C = A \cup (B \cup C)$. Pour cette raison, on peut oublier les parenthèses et noter ceci plus simplement $A \cup B \cup C$. C'est aussi la même chose que $C \cup B \cup A$, ou encore $A \cup C \cup B$, etc.

Si nous disposons d'une famille plus grande de sous-ensembles d'un ensemble donné E (fixé une fois pour toutes), disons $A_1, \ldots, A_n$ pour fixer les idées, on peut considérer leur union

$$A_1 \cup A_2 \cup \ldots \cup A_n := \bigcup_{i=1}^{n} A_i.$$

C'est l'ensembles des éléments x qui appartiennent à l'un des A_i, pour i de 1 à n. Le résultat ne dépend pas de l'ordre dans lequel on a énuméré ces ensembles. On peut obtenir cette union en réunissant les ensembles deux à deux dans n'importe quel ordre. Par exemple

$$A_1 \cup A_2 \cup A_3 \cup A_4 = (A_1 \cup A_2) \cup (A_3 \cup A_4) = ((A_1 \cup A_2) \cup A_3) \cup A_4 = A_1 \cup ((A_2 \cup A_3) \cup A_4) = \ldots.$$

Mais pourquoi s'arrêter à un nombre fini ? Supposons qu'on dispose d'une famille quelconque A_i de sous-ensembles de E, où i est un indice qui appartient lui même à un ensemble I. Alors, nous pouvons considérer l'ensemble $\bigcup_{i\in I} A_i$: c'est l'ensemble des éléments $x \in E$ pour lesquels il existe $i \in I$ tel que x appartient à l'un des A_i. En langage mathématique

$$x \in \bigcup_{i\in I} A_i \iff \exists i \in I,\ x \in A_i.$$

Le résultat ne dépend pas de l'ordre dans lequel sont donnés les A_i (d'ailleurs, quel sens ça aurait, d'énumérer les A_i lorsque I est un ensemble quelconque ?).

De la même manière, on peut considérer l'intersection des A_i, notée $\bigcap_{i\in I} A_i$: c'est l'ensemble des éléments $x \in E$ qui appartiennent à tous les A_i :

$$x \in \bigcap_{i\in I} A_i \iff \forall x \in I, x \in A_i.$$

Une fois de plus, le résultat ne dépend par de l'ordre des A_i.

On a comme pour les unions finies

$$\Big(\bigcup_{i\in I} A_i\Big)^c = \bigcap_{i\in I} A_i^c\ ;\ \Big(\bigcap_{i\in I} A_i\Big)^c = \bigcup_{i\in I} A_i^c.$$

1.2.2 Fonctions, applications

Lorsqu'on a deux ensembles A et B, (qui peuvent être les mêmes) une *application* entre A et B est une façon de faire correspondre à tout élément $a \in A$ un élément $f(a) \in B$.

Formellement, on peut la définir comme une relation entre A et B, c'est à dire une partie $\mathcal{F}$ de $A \times B$, qui est telle que pour tout point $a \in A$, il existe un unique $b \in B$ tel que $(a, b) \in \mathcal{F}$. Cette partie $\mathcal{F}$ de $A \times B$ s'appelle le graphe de la fonction f.

$$\mathcal{F} = \{(x, f(x)), x \in A\}.$$

A est l'ensemble de *départ*, et B l'ensemble d'*arrivée* de l'application f.

On appelle aussi souvent cette notion une *fonction* de A dans B. Pour nous, nous réserverons cette notion de fonction aux applications qui ne sont définies éventuellement que sur un sous-ensemble de A (qu'on appelle *l'ensemble de définition* de la fonction).

On note $f : A \to B$ et aussi $x \mapsto f(x)$.

Lorsque $y = f(x)$, on dit que y est *l'image* de x ou bien que que x est **un** *antécédent* de y. Attention à ce que, par définition, un point n'a qu'une image **mais peut avoir plusieurs antécédents**.

L'ensemble de toutes les applications de A dans B (c'est un ensemble !) se note $\mathcal{F}(A, B)$ ou encore B^A. Cette notation sera justifiée au chapitre Dénombrements où l'on montre que si A a n éléments et B a m éléments, alors B^A a m^n éléments.

Parmi les applications les plus simples, il y a l'*identité* $Id_E : E \to E$. C'est l'application qui à $x \in E$ fait correspondre $x \in E$ (elle ne fait rien !).

Les débutants ont souvent tendance à la confondre avec l'application constante qui à $x \in E$ fait correspondre toujours la même valeur $y \in F$.

Par exemple, l'application de $E = \{1, 2, 3\}$ dans lui même qui est telle que $f(1) = f(2) = f(3) = 1$ est constante, alors que pour l'identité, on a $f(1) = 1$, $f(2) = 2$, $f(3) = 3$.

Qu'est qu'on attend d'un étudiant lorsqu'on demande "Montrez que telle fonction f est bien une application de E dans F" ?

Cela dépend bien sûr du contexte. mais en général, il s'agit des points suivants.

(1) Tout d'abord que $f(x)$ est bien définie pour tout $x \in E$ (par exemple qu'on n'obtient pas $0/0$).

(2) Ensuite, que $f(x)$ est définie sans ambiguïté : par exemple, qu'il n'y a pas plusieurs valeurs possibles pour $f(x)$, comme par exemple "un réel tel que $x^2 = 1$".

(3) Enfin, que la valeur de $f(x)$ est bien dans l'ensemble F. Par exemple, la fonction $x \to x^2$ n'est une application de $\mathbb{R}$ dans $[0, 1]$, alors que c'est bien une application de $\mathbb{R} \to \mathbb{R}$ ou de $[-1, 1] \to [0, 1]$.

Retenir que deux applications f et g sont égales si et seulement si : elles ont même ensemble de départ, même ensemble d'arrivée et pour tout élément x de l'ensemble de départ, $f(x) = g(x)$.

Exercice 7. On considère trois applications f, g, h définies de $E := \{-1, 0, 1\}$ dans $\mathbb{R}$, par
- $f(-1) = 1$, $f(0) = 0$ et $f(1) = 1$,
- $\forall x \in E$, $g(x) = x^2$,
- $\forall x \in E$, $h(x) = x^4 - x^3 + x$.

Montrer que ces trois applications sont égales.

Il ne faut pas croire qu'une application est juste une formule !

Images et images réciproques d'ensembles

Lorsqu'on a une application $f : E \to F$, elle permet de définir de nouvelles applications $\mathcal{P}(E) \to \mathcal{P}(F)$ et $\mathcal{P}(F) \to \mathcal{P}(E)$ appelées images directes et réciproques, et qui sont les suivantes.

Image directe. Pour $A \subset E$, l'image directe $f(A)$ est l'ensemble des points de f qui sont images par f d'un point de A

$$f(A) = \{y \in F,\ \exists x \in A,\ y = f(x)\}.$$

Image réciproque Pour $B \subset F$, l'image réciproque $f^{-1}(B)$ est l'ensemble des points de E dont l'image est dans B (entre d'autres termes, c'est l'ensemble des antécédents des éléments de E)

$$f^{-1}(B) = \{x \in E,\ f(x) \in B\}.$$

L'image réciproque est une application très sympathique du point de vue de la théorie des ensembles

$$f^{-1}(A^c) = \left(f^{-1}(A)\right)^c,\ f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B),\ f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B).$$

De plus, si $A \subset B$, $f^{-1}(A) \subset f^{-1}(B)$.

Exercice 8. Démontrer les assertions qui précèdent.

Par contre, l'image directe est pleine de pièges, et nous invitons les lecteurs à s'en méfier ! ! ! Ainsi, on a

$$f(A \cap B) \subset f(A) \cap f(B),$$

mais l'inclusion inverse peut être fausse. De plus, il n'est pas vrai en général que $f(A^c) \subset f(A)^c$, ni que $f(A)^c \subset f(A^c)$.

Composition des applications

Lorsqu'on a deux applications $f : E \to F$ et $g : F \to G$, on peut considérer leur *composition*, qui est l'application $g \circ f : E \to G$ qui à $x \in E$ fait correspondre le point $g\big(f(x)\big) \in G$. (**Attention : l'écriture de la composition se fait à l'envers de la réprésentation** $E \to F \to G$.)

On a $h \circ (g \circ f) = (h \circ g) \circ f$. En d'autres termes, la composition des applications est **"associative"**. Nous avons déjà rencontré ce mot plus haut. Mais on n'a pas en général $f \circ g = g \circ f$ d'autant plus que ceci n'a aucun sens en général (sauf si $E = G$: pourquoi ?). La composition des application **n'est pas commutative**.

L'identité joue un rôle particulier pour la composition. En effet, si on a une application $f : E \to F$, on a $f \circ Id_E = f$ et $Id_F \circ f = f$.

Restriction d'une application

Etant donnés une application $f : E \mapsto F$ et un sous-ensemble $A \subset E$, on peut considérer l'application $f_{|A} : A \to F$ qui à $x \in A$ associe $f(x) \in F$. C'est la *restriction* (au départ) de f à A.

Si un sous-ensemble $B \subset F$ vérifie $f(E) \subset B$, alors on peut construire la restriction à l'arrivée de f à B (attention, dans ce cas, il y a une condition sur B). C'est l'application de $E \to B$ qui a tout $x \in E$ associe $f(x) \in B$. Le plus petit B qu'on puisse choisir est $f(E)$. On peut noter cette nouvelle application $f^{|B}$.

Si $f(A) \subset B$ on peut restreindre f à la fois au départ à A et à l'arrivée à B.

Calculer avec des ensembles.

Il est parfois fastidieux de vérifier des identités entre ensembles. Il est alors commode de remplacer le calcul sur les ensembles par du calcul algébrique. Pour cela, introduisons la notion d'indicatrice d'un sous-ensemble (aussi appelée fonction caractéristique) d'un ensemble E. Jusqu'à la fin de ce paragraphe, tous les ensembles considérés seront des sous-ensembles de E. Si $A \subset E$, alors 1_A est la fonction $f : E \to \{0, 1\}$ telle que $f(x) = 1$ si $x \in A$ et $f(x) = 0$ si $x \in A^c$.

En notant $1 = 1_E$ la fonction constante égale à 1 sur E, on a $1_{A^c} = 1 - 1_A$ et $1_{A \cap B} = 1_A 1_B$ (c'est-à-dire le produit terme à terme des fonctions 1_A et 1_B). On en déduit par exemple :

$$1_{A \cup B} = 1_{(A^c \cap B^c)^c} = 1 - (1 - 1_A)(1 - 1_B) = 1_A + 1_B - 1_{A \cap B}.$$

Ensuite, pour montrer l'identité de deux ensembles, il suffit de montrer l'égalité de leurs indicatrices.

Par exemple, si l'on veut montrer que $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$, (c'est-à-dire la distributivité de $\cup$ par rapport à $\cap$) en prenant les indicatrices, nous trouvons pour le premier terme

$$1_{(A \cap B) \cup C} = 1_{A \cap B} + 1_C - 1_{A \cap B \cap C},$$

tandis que pour le deuxième, nous avons

$$\begin{aligned} 1_{(A \cup C) \cap (B \cup C)} &= \Big(1_A + 1_C - 1_{A \cap C}\Big)\Big(1_B + 1_C - 1_{B \cap C}\Big) \\ &= 1_{A \cap B} + 1_{A \cap C} - 1_{A \cap B \cap C} \\ &+ 1_{B \cap C} + 1_C - 1_{B \cap C} \\ &- (1_{A \cap B \cap C} + 1_{A \cap C} - 1_{A \cap B \cap C}), \end{aligned}$$

et c'est bien la même chose.

Exercices

Exercice 9. Complétez le tableau suivant (à chaque ligne les valeurs des énoncés P et Q sont indiquées par les deux premières cases, à vous de donner la valeur des autres énoncés).

P	Q	$nonP$	$P \wedge Q$	$P \vee Q$	$P \Longrightarrow Q$	$P \iff Q$	$(P \wedge nonQ) \vee (Q \wedge nonP)$
$vrai$	$vrai$						
$vrai$	$faux$						
$faux$	$vrai$						
$faux$	$faux$						

Exercice 10. Dans l'ensemble $\mathbb{N}$ des entiers naturels, lesquels de ces énoncés sont vrais ?

(1) $\exists y, \forall x > y, x \leq 1$.

(2) $\exists y, \forall x > y, x \geq 1$.

(3) $\exists y, \forall x < y, x \leq 1$.

(4) $\exists y, \forall x < y, x \geq 1$.

(5) $\forall x, \exists y > x, \forall z < y, z \leq x$.

(6) $\forall x, \exists y > x, \forall z < y, z < x$.

Exercice 11. (*) Dans l'ensemble $\mathbb{N}$ des entiers naturels, trouvez lorsqu'elles existent les valeurs de a pour lesquelles les propositions suivantes sont vraies

(1) $\forall x \leq 3, \exists y \leq a, x \leq y$

(2) $\exists y \leq a, \forall x \leq 3, x \leq y$

(3) $\forall x \leq a, \exists y \leq 3, x \leq y$

(4) $\exists y \leq 3, \forall x \leq a, x \leq y$

Exercice 12. Donnez la négation des énoncés suivants

(1) $\forall x \geq 2, \exists y \leq a, y \leq x$

(2) $A \Longrightarrow B$

(3) $A \iff B$

(4) $\exists p \in \mathbb{N}^*$, $\exists n_0 \in \mathbb{N}$, $\forall n \geq n_0, u_{n+p} = u_n$. Quel est le sens de cet énoncé ?

(5) (*) J'ai lu tous les livres de math de la BU qui contiennent moins de 300 pages et dont le titre commence par M.

Exercice 13. Ecrire $\mathcal{P}(A)$ pour $A = \{1, 2, 3\}$, et pour $A = \mathcal{P}(\{\emptyset\})$.

Exercice 14. Soient A, B des ensembles.

(1) Montrer que $A = (A \cap B) \cup (A \setminus B)$ et que $(A \cap B) \cap (A \setminus B) = \emptyset$. En déduire une partition de A.

(2) Montrer que $A \cup B = A \cup (B \setminus A)$ et $A \cap (B \setminus A) = \emptyset$. En déduire une partition de $A \cup B$.

Exercice 15. On définit pour tout $n \in \mathbb{N}$ l'ensemble $I_n = \{0, \ldots, n\}$ et $J_n = \{n, n+1, \ldots\} = \{i \in \mathbb{N};\ i \geq n\}$.

(1) Parmi les ensembles $I_n, J_n, I_{n+1}, J_{n+1}$, qui est inclus dans qui ? Lesquels sont disjoints ?

(2) Calculez les ensembles

$$\bigcup_{n\in\mathbb{N}} I_n, \quad \bigcap_{n\in\mathbb{N}} I_n, \quad \bigcup_{n\in\mathbb{N}} J_n, \quad \bigcap_{n\in\mathbb{N}} J_n.$$

Exercice 16. (**) On considère un ensemble E et, pour tout entier $n \geq 1$, on se donne un sous-ensemble A_n de E.

On définit pour tout $n \geq 1$ les sous-ensembles $\overline{A}_n = \cup_{p=n}^{\infty} A_p$ et $\underline{A}_n = \cap_{p=n}^{\infty} A_p$

(1) Montrez que pour tout $n \geq 1$, $\underline{A}_n \subset \overline{A}_n$.

(2) Montrez que pour tout $n \geq 1$, $\overline{A}_{n+1} \subset \overline{A}_n$.

(3) Montrez que pour tout $n \geq 1$, $\underline{A}_n \subset \underline{A}_{n+1}$.

(4) On définit $\overline{A} = \cap_{n=1}^{\infty} \overline{A}_n$ et $\underline{A} = \cup_{n=1}^{\infty} \underline{A}_n$. Montrez que $\underline{A} \subset \overline{A}$.

(5) Montrez que $\overline{A}$ est l'ensemble de tous les éléments x qui appartiennent à une infinité de A_n.

(6) Montrez que $\underline{A}$ est l'ensemble de tous les éléments x qui appartiennent à tous les A_n à partir d'un certain rang.

(7) Montrez que si, $\forall n, A_n \subset A_{n+1}$, alors $\underline{A} = \overline{A}$.

(8) Montrez que si, $\forall n, A_{n+1} \subset A_n$, alors $\underline{A} = \overline{A}$.

Exercice 17. Avec $E = \{1, 2\}$, donnez deux applications f et g de E dans lui-même telles que $f \circ g \neq g \circ f$.

Exercice 18. Trouver un exemple où $A \cap B = \emptyset$ et où $f(A) \cap f(B) \neq \emptyset$.

Exercice 19. (*) Trouver un exemple où les inclusions $f(A^c) \subset f(A)^c$ et $f(A)^c \subset f(A^c)$ sont fausses.

Exercice 20. Lorsque $f : E \to F$ est une application, montrer que $\{f^{-1}(\{y\}), y \in f(E)\}$ forme une partition de E.

(*) Réciproquement, montrer qu'une partition de E peut toujours être réalisée de cette manière.

Exercice 21. (*) La différence symétrique de deux ensembles A et B est l'ensemble

$$A \Delta B := \big(A \setminus B\big) \cup \big(B \setminus A\big).$$

(1) On a vu en cours que l'union d'ensembles correspond au connecteur logique $\vee$ (ou inclusif). A quelle opération logique correspond Δ ?

(2) Montrez que $1_{A\Delta B} = (1_A - 1_B)^2$. En déduire que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

Exercice 22. Soit $f : E \to E$ une application. On définit les *itérées* de f par récurrence : $f^{(0)} := \mathrm{Id}_E$ (application identité de E) et pour tout $n \in \mathbb{N}$, $f^{(n+1)} = f \circ f^{(n)}$. Par exemple $f^{(1)} = f \circ \mathrm{Id}_E = f$, $f^{(2)} = f \circ f$.

(1) Prouver par récurrence sur n que $\forall n, p \in \mathbb{N}$, $f^{(n+p)} = f^{(n)} \circ f^{(p)}$

(2) On prend $E = \mathbb{N}$ et $f(x) = x + 1$. Que vaut $f^{(n)}(x)$?

(3) On prend $E = \mathbb{N}$ et $f(x) = 2x$. Que vaut $f^{(n)}(1)$?

Chapitre 2

Dénombrements

Référence pour ce chapitre : le module II.1 du L1, section 2.2.

2.1 Les bases

Nous commençons par présenter en détail des outils indispensables au dénombrement des ensembles.

2.1.1 Principes de récurrence

Rappelons que l'ensemble $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ des entiers naturels est muni des opérations d'addition et de multiplication, mais aussi de la relation d'ordre $\leq$ (inférieur ou égal) qui possède la propriété fondamentale suivante :
Toute partie non vide de $\mathbb{N}$ *admet un plus petit élément* [1].

On peut déduire de cette propriété de $\mathbb{N}$ le *principe de récurrence*. Dans la pratique, on considère ce principe comme une méthode de démonstration. Celle-ci admet au moins trois formes distinctes, que nous allons expliciter et illustrer. On considère un énoncé $P(n)$ qui dépend d'un nombre entier n ; on cherche à montrer qu'il est vrai pour tout $n \geq n_0$ (en pratique n_0 vaudra souvent 0 ou 1).

La preuve par *récurrence simple* est celle-ci :
Soit $P(n)$ un énoncé défini sur $\mathbb{N}$ (pour $n \geq n_0$ suffit) et vérifiant les deux hypothèses suivantes :
- *Initialisation : $P(n_0)$ est vrai.*
- *Hérédité : $\forall n \geq n_0$, $\big(P(n) \Rightarrow P(n+1)\big)$.*

Alors P est vrai pour tout entier n supérieur ou égal à n_0 : $\forall n \geq n_0,\ P(n)$.

Exemple.
Montrons que, pour tout $n \in \mathbb{N}$, on a $2^n \geq n + 1$. Nous notons donc, pour tout $n \in \mathbb{N}$:

$$P(n) := (2^n \geq n + 1).$$

Initialisation : la propriété $P(0)$ dit que $2^0 \geq 1$, *i.e.* que $1 \geq 1$, qui est vraie.
Hérédité : supposons $P(n)$ vraie, *i.e.* $2^n \geq n + 1$ (hypothèse de récurrence). Alors :

$$2^{n+1} = 2 \times 2^n \geq 2(n + 1) = 2n + 2 \geq (n + 1) + 1.$$

[1] On dit que cette relation d'ordre fait de $\mathbb{N}$ un ensemble "bien ordonné".

La première inégalité utilisait l'hypothèse de récurrence. On a bien prouvé $P(n+1)$. Du principe de récurrence (simple), on déduit que $\forall n \in \mathbb{N}\ ,\ P(n)$.

La preuve par *récurrence double*, ou *récurrence à deux pas* [2] repose sur le principe suivant :
Soit $P(n)$ un énoncé défini sur $\mathbb{N}$ et vérifiant les deux hypothèses suivantes :

- *Initialisation : $P(n_0)$ et $P(n_0+1)$ sont vrais.*
- *Hérédité : $\forall n \geq n_0\ ,\ \Big(\big(P(n)\ et\ P(n+1)\big) \Rightarrow P(n+2)\Big)$.*

Alors P est vrai sur $\mathbb{N}$ tout entier supérieur ou égal à n_0 : $\forall n \geq n_0\ ,\ P(n)$.

Exemple.
Nous allons démontrer que $(1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbb{N}$ pour tout entier $n \in \mathbb{N}$. C'est vrai pour $n=0$ et $n=1$ (calcul facile). En remarquant que $1+\sqrt{2}$ et $1-\sqrt{2}$ sont solutions de l'équation $X^2 = 2X+1$, il vient

$$\begin{aligned}
&(1+\sqrt{2})^{n+2} + (1-\sqrt{2})^{n+2} \\
&= (1+\sqrt{2})^n(1+\sqrt{2})^2 + (1-\sqrt{2})^n(1-\sqrt{2})^2 \\
&= (1+\sqrt{2})^n\big(2(1+\sqrt{2})+1\big) + (1-\sqrt{2})^n\big(2(1-\sqrt{2})+1\big) \\
&= 2\big((1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\big) + \big((1+\sqrt{2})^n + (1-\sqrt{2})^n\big),
\end{aligned}$$

ce que l'on peut écrire $u_{n+2} = 2u_{n+1} + u_n$, en posant $u_n := (1+\sqrt{2})^n + (1-\sqrt{2})^n$. Il est alors clair que ($u_n \in \mathbb{N}$ et $u_{n+1} \in \mathbb{N}$) $\Rightarrow u_{n+2} \in \mathbb{N}$, et l'on a bien l'hérédité, donc la conclusion par récurrence à deux pas.

L'hérédité dans cette démonstration, repose sur la relation (de récurrence à deux pas !) $u_{n+2} = 2u_{n+1} + u_n$. Notons qu'en posant $v_n := (1+\sqrt{2})^n - (1-\sqrt{2})^n$ on a la relation analogue : $v_{n+2} = 2v_{n+1} + v_n$, donc la même propriété d'hérédité pour l'assertion $v_n \in \mathbb{Z}$. De plus, cette dernière est vraie pour $n=0$, mais fausse pour $n=1$: l'initialisation en $n=0$ est donc insuffisante dans une récurrence à deux pas.

Enfin, nous présentons le principe de preuve par *récurrence complète*, qui est aussi appelée *récurrence forte* :
Soit $P(n)$ un énoncé défini sur $\mathbb{N}$ ($n \geq n_0$ suffit) et vérifiant les hypothèses suivantes :

- *Initialisation : $P(n_0)$ est vrai.*
- *Hérédité :*

$$\forall n \geq n_0\ ,\ \Big(\big(\forall m \in \mathbb{N}\ tel\ que\ n_0 \leq m \leq n\ ,\ P(m)\big) \Rightarrow P(n+1)\Big).$$

Alors P est vrai pour $\mathbb{N}$ tout entier n supérieur ou égal à n_0 : $\forall n \in \mathbb{N}\ ,\ P(n)$.

Exemple.
Disons qu'un entier $n \in \mathbb{N} \setminus \{0,1\}$ est *irréductible* s'il n'est pas le produit de deux entiers $p, q \in \mathbb{N} \setminus \{0,1\}$. Nous allons montrer que tout entier de $\mathbb{N} \setminus \{0,1\}$ (c'est-à-dire supérieur ou égal à $n_0 := 2$) est produit d'entiers irréductibles.
Nous notons donc, pour tout $n \in \mathbb{N} \setminus \{0,1\}$:

$$P(n) := (n \text{ est produit d'entiers irréductibles}).$$

Initialisation : si n s'écrit comme $n = pq$ avec $p, q \geq 2$ alors $n \geq 4$. Donc 2 est irréductible (3 aussi !)

[2] Il existe aussi des récurrence à trois pas, et même à k pas, où $k \in \mathbb{N}^*$.

Hérédité forte : Soit $n \geq 2$. Supposons que tout entier m avec $2 \leq m \leq n$ vérifie $P(m)$, autrement dit, qu'il est produit d'irréductibles. Il s'agit d'en déduire que $n+1$ est lui-même produit d'irréductibles. On distingue deux cas :

(1) Si $n+1$ est irréductible, il est bien entendu produit d'irréductibles !

(2) Sinon, il est réductible et l'on peut écrire $n+1 = pq$ avec $p, q \in \mathbb{N} \setminus \{0, 1\}$. Comme $p, q > 1$, on a $p, q < n+1$ donc $2 \leq p, q \leq n$. On peut donc leur appliquer l'hypothèse de récurrence forte : $P(p)$ et $P(q)$ sont vraies, *i.e.* p et q sont produits d'irréductibles, donc $n+1 = pq$ aussi.

On a bien démontré $P(n)$, donc l'hérédité forte. Du principe de récurrence forte on tire la conclusion. (Cette démonstration remonte aux Éléments d'Euclide.)

Constructions par récurrence. On peut *définir* des objets par récurrence. Il y a, là encore, les récurrences simple, à deux (ou k) pas et la récurrence forte. Nous allons illustrer chaque cas par un exemple.

Exemple.
On peut définir une suite numérique par récurrence simple. C'est le cas de la suite des *factorielles* :

$$0! := 1 \text{ et } \forall n \in \mathbb{N}\ ,\ (n+1)! := (n+1)\, n!.$$

Ainsi, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, etc.

Exemple.
La célèbre suite de Fibonacci est définie par récurrence double :

$$F_0 = 0,\ F_1 := 1 \text{ et } \forall n \in \mathbb{N}\ ,\ F_{n+2} := F_{n+1} + F_n.$$

Exemple.
On peut aussi définir une suite numérique par récurrence complète, par exemple : $u_0 = 1$ et

$$\forall n \in \mathbb{N}^*\ ,\ u_n := 1 + \sum_{i=0}^{n-1} u_i.$$

On a donc $u_0 = 1$, $u_1 = 2$, $u_2 = 4$, $u_3 = 8$ et ensuite ?

Exercice 23. Démontrer par récurrence sur n que dans l'exemple précédent, $u_n = 2^n$.

Exercice 24. (*) Démontrez le principe de récurrence simple en utilisant la propriété "un sous-ensemble de $\mathbb{N}$ qui n'est pas vide admet un plus petit élément". On pourra considérer l'ensemble $\{n \geq n_0;\ P(n) \text{ est faux}\}$.

2.1.2 Injections, surjections, bijections

Les définitions qui suivent sont **absolument fondamentales**. Il est indispensable de bien les comprendre pour la suite du cours.

Définition. *On dit qu'une fonction $f : E \to F$ est* injective *si tout point $y \in F$ a* **au plus** *un antécédent. On dit aussi que f est* une injection. *Autrement dit*

$$(f(x_1) = f(x_2)) \Longrightarrow x_1 = x_2,$$

ou encore par contraposition

$$(x_1 \neq x_2) \Longrightarrow (f(x_1) \neq f(x_2)).$$

L'exemple le plus simple d'injection s'obtient lorsqu'on a un ensemble E et une partie $A \subset E$. Alors, l'application $f : A \to E$ donnée par $f(x) = x$ est une injection. On l'appelle *l'injection canonique* de A dans E.

Définition. *On dit qu'une fonction $f : E \to F$ est* surjective *si tout point $y \in F$ a* **au moins** *un antécédent. On dit aussi que f est* une surjection. *En d'autres termes, $f : E \to F$ et surjective si et seulement si $f(E) = F$.*

Lorsqu'on a $A \subset E$, on peut fabriquer une surjection $f : E \to A$ en choisissant d'abord un point $a \in A$, puis en considérant la fonction définie de la façon suivante : si $x \in A$, $f(x) = x$, et si $x \notin A$, $f(x) = a$.

Définition. *Lorsqu'une application $f : E \to F$ est à la fois injective et surjective, on dit qu'elle est* bijective*, ou que c'est* une bijection. *En d'autres termes, tout $y \in F$ admet* **un unique** *antécédent.*

L'exemple le plus simple de bijection est $Id_E : E \to E$.

Définition. *Soit $f : E \to F$ une bijection. On définit alors son* application réciproque *comme ceci : c'est l'application de F dans E qui à tout $y \in F$ associe son unique antécédent pour f. On la note f^{-1} et elle vérifie $f^{-1} \circ f = \mathrm{Id}_E$ et $f \circ f^{-1} = \mathrm{Id}_F$.*

Ces deux égalités sont plus une propriété qu'une définition et elles méritent d'être justifiées : pour tout $x \in E$, $f^{-1}(f(x))$ est par définition l'unique antécédent de $f(x)$ par f ; c'est donc x et on a bien $f^{-1}(f(x)) = x$. Pour $y \in F$, comme $f^{-1}(y)$ est l'antécédent de y, $f(f^{-1}(y)) = y$.

Une autre manière de traduire ces relations :

$$y = f(x) \iff x = f^{-1}(y).$$

Ceci montre en particulier que f^{-1} est aussi bijective et que $(f^{-1})^{-1} = f$ (la réciproque de la réciproque est la fonction elle-même).

Nous aurons besoin de la propriété suivante qui relie ces notions avec la composition d'applications :

Proposition 1. *Soient $f : E \to F$ et $g : F \to G$ deux applications.*

(1) Si $g \circ f$ est injective, alors f est injective.

(2) Si $g \circ f$ est surjective, alors g est surjective.

(3) Si $g \circ f$ est bijective, alors f est injective et g est surjective.

Démonstration. Pour le premier point : si $x, y \in E$ vérifient que $f(x) = f(y)$, alors en appliquant g on obtient $g(f(x)) = g(f(y))$, c'est-à-dire $(g \circ f)(x) = (g \circ f)(y)$. Comme $g \circ f$ est injective on peut conclure que $x = y$. Nous avons bien montré $(f(x) = f(y)) \Longrightarrow (x = y)$.

Pour le deuxième point : soit $z \in G$. Par hypothèse, $g \circ f$ est surjective, donc il existe $x \in E$ tel que $z = (g \circ f)(x) = g(f(x))$. Ainsi z admet un antécédent pour g (c'est $f(x)$, il y en a peut être d'autres d'ailleurs).

Le dernier point est la conjonction des deux premiers. □

Exercice 25. Démontrer que la composition de deux injections est une injection, et que la composition de deux surjections est une surjection. Et pour les bijections ?

Les notions d'injection, surjection et bijection sont essentielles pour le dénombrement. En particulier, si $f : E \to F$ est une bijection, elle définit une correspondance entre les éléments de E et F : à tout élément de E correspond un élément de F et réciproquement. Donc, intuitivement, les deux ensembles ont le même nombre d'éléments. Le résultat suivant, qui permet d'établir facilement que des applications sont des bijections, nous sera très utile en pratique.

Théorème 2.1.1. *Si $f : E \to F$ et $g : F \to E$ sont deux applications telles que $g \circ f = Id_E$ et $f \circ g = Id_F$, alors ces deux applications sont bijectives et $f = g^{-1}$, $g = f^{-1}$.*

Démonstration. Puisque $g \circ f = Id_E$ est bijective, nous savons par la proposition 1 que g est surjective et f est injective. De même, nous savons que $f \circ g$ est bijective et donc que f est surjective et g injective. Donc, f et g sont bijectives et par conséquent, elles admettent des applications réciproques f^{-1} et g^{-1}. Finalement on obtient par composition

$$f^{-1} = Id_E \circ f^{-1} = (g \circ f) \circ f^{-1} = g \circ (f \circ f^{-1}) = g \circ Id_F = g.$$

$$g^{-1} = Id_F \circ g^{-1} = (f \circ g) \circ g^{-1} = f \circ (g \circ g^{-1}) = f \circ Id_E = f.$$

□

Exercice 26. Supposons que $f : E \to F$ et $g : F \to G$ sont des bijections. Montrer que $g \circ f : E \to G$ est bijective d'application réciproque $f^{-1} \circ g^{-1}$.

Attention : il ne faut pas confondre l'application réciproque f^{-1} avec l'application "image réciproque d'une ensemble" $A \mapsto f^{-1}(A)$, bien qu'on utilise la même notation pour les deux notions.

Bien qu'on dispose de deux notions pour f^{-1}, les choses ne sont pas si affreuses que ça. Après tout, on disposait aussi de deux notions pour f : image d'un point ou bien image directe d'un ensemble. Lorsque $f : E \to F$ est bijective, et que $B \subset F$ est un sous-ensemble de F, alors l'image réciproque $f^{-1}(B)$ est aussi l'image directe de B par l'application $f^{-1} : F \to E$. Si bien que les deux notions (apparemment différentes) de $f^{-1}(B)$ décrivent en fait le même sous-ensemble de E.

Exercice 27. (*) Démontrer l'assertion qui précède.

2.2 Cardinaux finis.

La notion de cardinal d'un ensemble fini est claire : c'est le nombre d'éléments qu'il contient. Cette définition intuitive est un peu vague du point de vue mathématique. Nous allons en proposer une plus formelle, pas simplement par souci de rigueur, mais parce qu'elle indique une méthode de dénombrement utilisable en pratique. Dans la suite on note $[\![1, n]\!] := \{1, \ldots, n\}$ l'ensemble des entiers naturels compris, au sens large, entre 1 et n.

Définition. *Un ensemble est dit* fini *s'il est vide ou s'il existe un entier $n \geq 1$ et une bijection $f : [\![1, n]\!] \to E$. Le* cardinal *d'un ensemble fini E, noté* card E *vaut 0 si $E = \emptyset$ et n dans le cas où il existe une bijection $f : [\![1, n]\!] \to E$.*

Remarquons que dans ce dernier cas, on peut écrire $E = \{f(1), \ldots, f(n)\}$. Cette définition correspond donc à ce que l'on fait lorsque l'on compte des objets : on leur attribue (dans un ordre arbitraire) les numéros 1,2,3, etc, en veillant à ne pas compter deux fois le même objet (c'est l'injectivité de f) et à n'oublier aucun objet (surjectivité de f).

Nous présentons d'abord des résultats généraux sur les cardinaux et les appliquons ensuite de manière amusante. Dans ce qui suit, tous les ensembles sont finis.

Théorème 2.2.1. *Soit $f : E \to F$ une application entre ensembles finis.*

(1) Si f est bijective, alors card $E =$ card F.

(2) Si f est injective, alors card $E \leq$ card F.

(3) Si f est surjective, alors card $E \geq$ card F.

(4) On suppose que card $E =$ card F. *Alors f est injective si, et seulement si, elle est surjective. (Naturellement dans ce cas elle est alors bijective.)*

□

Comme ces résultats sont intuitivement évidents, nous n'allons pas les démontrer à partir de la définition formelle (afin de ne pas donner l'impression d'enfonçer les portes ouvertes. Le lecteur pourra les démontrer pour s'entraîner ; le premier point est facile, les suivants nécessitent des récurrences et peut-être des étoiles). Nous allons plutôt en tirer des conséquences. Il faut retenir qu'**un moyen fondamental de démontrer que deux ensembles ont le même nombre d'éléments est d'exhiber une bijection entre les deux**. De même pour montrer que l'ensemble E n'a pas plus d'élements que F, il suffit d'exhiber une injection de E dans F ; pour montrer que E a au moins autant d'élements que F, il suffit d'exhiber une surjection de E sur F.

Une conséquence remarquable est que si E est fini, toute injection de E dans E est automatiquement bijective. Cette propriété est n'est plus vraie pour les ensembles infinis : par exemple l'application $n \mapsto n + 1$ de $\mathbb{N}$ dans $\mathbb{N}$ est injective mais 0 n'est pas dans l'image.

Par contraposition, le second point du théorème donne le résultat suivant, connu sous le nom de "Principe des tiroirs de Dirichlet" (et "pigeonhole principle" en anglais ! !)

Corollaire 2.2.2. *Soit $f : E \to F$ une application. Si* card $E >$ card F, *il existe $a \neq b \in E$ tels que $f(a) = f(b)$.*

Exemples.
Dans un groupe de 27 personnes, il y en a certainement deux dont le nom commence par la même lettre.
Le nombre de cheveux normal d'une personne (pas trop chauve) est de l'ordre de 100000 à 150000. Admettons qu'il soit toujours inférieur à 200000. Il y a donc à Toulouse deux personnes qui ont le même nombre de cheveux.

2.2.1 Union d'ensembles, addition de cardinaux

Nous prendrons comme point de départ la propriété suivante :
Si A et B sont des ensembles finis disjoints, card $(A \cup B) =$ card $A +$ card B.

Théorème 2.2.3. *Si A et B sont des ensembles finis quelconques :*

$$\text{card } (A \cup B) = \text{card } A + \text{card } B - \text{card } (A \cap B).$$

Démonstration. On a d'abord, par application de la propriété de départ à la réunion disjointe $A = (A \cap B) \cup (A \setminus B)$, établie à l'exercice 14 :

$$\text{card } A = \text{card } (A \cap B) + \text{card } (A \setminus B) \Longrightarrow \text{card } A - \text{card } (A \cap B) = \text{card } (A \setminus B).$$

On remarque ensuite que $(A \cup B)$ est l'union disjointe de B et de $(A \setminus B)$, auxquels on applique à nouveau la propriété de départ :

$$\text{card } (A \cup B) = \text{card } B + \text{card } (A \setminus B) = \text{card } A + \text{card } B - \text{card } (A \cap B).$$

□

Essayons le cas de trois ensembles finis A, B, C, en utilisant ce que nous savons pour la réunion de deux ensembles :

$$\text{card } (A \cup B \cup C) = \text{card } \big((A \cup B) \cup C\big) = \text{card } (A \cup B) + \text{card } (C) - \text{card } \big((A \cup B) \cap C\big).$$

On calcule donc card $(A \cup B) = \text{card } A + \text{card } B - \text{card } (A \cap B)$ et :

$$\begin{aligned} \text{card } \big((A \cup B) \cap C\big) &= \text{card } \big((A \cap C) \cup (B \cap C)\big) \\ &= \text{card } (A \cap C) + \text{card } (B \cap C) - \text{card } \big((A \cap C) \cap (B \cap C)\big) \\ &= \text{card } (A \cap C) + \text{card } (B \cap C) - \text{card } (A \cap B \cap C). \end{aligned}$$

En reportant dans la première égalité, on trouve enfin :

$$\text{card } (A \cup B \cup C) = \text{card } A + \text{card } B + \text{card } C - \text{card } (A \cap B) - \text{card } (A \cap C) - \text{card } (B \cap C) + \text{card } (A \cap B \cap C).$$

Cette formule se généralise à une union de n ensembles, pour n quelconque :

Théorème 2.2.4 (Formule d'inclusion-exclusion ou formule du crible)**.** *Soient $A_1, \ldots, A_n$ des ensembles finis quelconques. Alors :*

$$\begin{aligned} \text{card } (A_1 \cup \cdots \cup A_n) &= \sum_{i=1}^{n} \text{card } A_i - \sum_{1 \le i < j \le n} \text{card } (A_i \cap A_j) \\ &+ \sum_{1 \le i < j < k \le n} \text{card } (A_i \cap A_j \cap A_k) \\ &- \sum_{1 \le i < j < k < \ell \le n} \text{card } (A_i \cap A_j \cap A_k \cap A_\ell) + \cdots \\ &+ (-1)^{n-1} \text{card } (A_1 \cap \cdots \cap A_n) \\ &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le n} \text{card } (A_{i_1} \cap \cdots \cap A_{i_k}). \end{aligned}$$

Démonstration. Par récurrence sur n ; réservé aux courageux ! □

Exemple.
Anticipant sur le cours d'arithmétique, nous allons calculer le nombre d'entiers dans $[\![1, 900]\!]$ ayant un facteur commun avec 900. Ces entiers sont nécessairement divisibles par l'un des facteurs premiers de 900, lesquels sont 2, 3 et 5. On pose donc :

$$A := \{n \in [\![1, 900]\!] \mid 2|n\}, \quad B := \{n \in [\![1, 900]\!] \mid 3|n\} \text{ et } C := \{n \in [\![1, 900]\!] \mid 5|n\}.$$

Les éléments de A sont les $2k$ tels que $1 \le k \le 900/2$, il y en a donc 450 ; avec le même raisonnement pour B et C, on trouve :

$$\text{card } A = 450, \quad \text{card } B = 300 \text{ et card } C = 180.$$

Les éléments de $A \cap B$ sont les $6k$ tels que $1 \leq k \leq 900/6$, il y en a donc 150 ; avec le même raisonnement pour $A \cap C$ et $B \cap C$, on trouve :

$$\text{card } (A \cap B) = 150, \quad \text{card } (A \cap C) = 90 \text{ et card } (B \cap C) = 60.$$

Enfin, les éléments de $A \cap B \cap C$ sont les $30k$ tels que $1 \leq k \leq 900/30$, il y en a donc 30. Finalement, le nombre cherché est :

$$\begin{aligned} \text{card } (A \cup B \cup C) &= \text{card } A + \text{card } B + \text{card } C \\ &- \text{card } (A \cap B) - \text{card } (A \cap C) - \text{card } (B \cap C) \\ &+ \text{card } (A \cap B \cap C) \\ &= 450 + 300 + 180 - 150 - 90 - 60 + 30 = 660. \end{aligned}$$

Il est important de retenir le cas particulier suivant, qui se démontre simplement par récurrence à partir de $(A \cap B = \emptyset) \Longrightarrow (\text{card } (A \cup B) = \text{card } (A) + \text{card } (B))$.

Proposition 2. *Soient $A_1, \ldots, A_n$ des ensembles finis deux à deux disjoints ($i \neq j \Longrightarrow A_i \cap A_i = \emptyset$), alors*

$$\text{card } \left(\bigcup_{i=1}^{n} A_i \right) = \sum_{i=1}^{n} \text{card } (A_i).$$

Remarque importante sur les sommes : La formule ci-dessus fait intervenir une expression de la forme $\sum_{i=1}^{n} u_i = u_1 + \cdots + u_n$, qui pour être précis, est définie par récurrence : $\sum_{i=1}^{1} u_i := u_1$ et pour tout $n \geq 1$, $\sum_{i=1}^{n+1} u_i = \left(\sum_{i=1}^{n} u_i \right) + u_{n+1}$. Il est utile de généraliser la notion de somme finie. Voici le cadre : on considère un ensemble fini A et une application $f : A \to \mathbb{R}$. On définit la somme sur $a \in A$ des $f(A)$ comme ceci : si A est vide la somme vaut 0 par convention, sinon en notant $n = \text{card } (A) \geq 1$, il existe par définition une bijection $\varphi : [\![1, n]\!] \to A$. On pose alors la définition suivante

$$\sum_{a \in A} f(a) := \sum_{i=1}^{n} f(\varphi(i)) = f(\varphi(1)) + \cdots + f(\varphi(n)).$$

La bijection φ nous fournit ainsi un ordre dans lequel on ajoute les nombres $f(a)$, mais par commutativité de l'addition, le résultat ne dépend pas de l'ordre (c'est un bon exercice de le démontrer par récurrence sur n). Donc la quantité définie ne dépend pas du choix de la bijection particulière φ que l'on a pu choisir. Nous allons donner sans détailler les arguments, des conséquences pratiques qui serviront pour traiter les exercices :

– Ce que l'on vient de dire montre que si $\psi : A \to A$ est bijective alors

$$\sum_{a \in A} f(a) = \sum_{b \in A} f(\psi(b)).$$

Les variables a et b sont muettes (nous aurions pu écrire a à la place de b dans la formule de droite). Cette règle revient à effectuer un changement de variable $a := \psi(b)$ dans la somme, donc un changement de l'ordre des termes qui ne modifie pas la valeur de la somme. Un exemple plus concret : en posant $i = n - k + 1$, on a

$$\sum_{i=1}^{n} u_i = \sum_{i=1}^{n} u_{n-i+1}$$

qui signifie $u_1 + u_2 + \cdots + u_n = u_n + u_{n-1} + \cdots + u_1$.

– Présentons un autre exemple de ce principe, tout aussi utile pour les calculs : l'interversion de sommes (finies) :

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_{i,j}\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{i,j}\right).$$

Si on note $I := [\![1, m]\!]$, $J := [\![1, n]\!]$ et $f : I \times J \to \mathbb{R}$ telle que $f(i, j) = a_{i,j}$, on se rend compte que les deux quantités qui précèdent valent

$$\sum_{x \in I \times J} f(x),$$

mais qu'elles correspondent à deux manières différentes d'énumérer les éléments de $I \times J$. Dans l'exemple concret $I = \{1, 2\}$, $J = \{1, 2, 3\}$ la formule d'interversion dit simplement que

$$(a_{1,1} + a_{1,2} + a_{1,3}) + (a_{2,1} + a_{2,2} + a_{2,3}) = (a_{1,1} + a_{2,1}) + (a_{1,2} + a_{2,2}) + (a_{1,3} + a_{2,3}).$$

– Si $A \subset E$ sont des ensembles finis et $1_A : E \to \{0, 1\}$ est la fonction caractéristique de A ($1_A(x)$ vaut 1 si $x \in A$ et 0 si $x \notin A$). Alors on a la relation

$$\text{card } A = \sum_{x \in E} 1_A(x),$$

qui est évidente si on y réfléchit puisque l'on compte 1 pour chaque élément de A.

– Pour finir nous reformulons la proposition 2 dans le cadre des sommes sur les ensembles : Soit I un ensemble fini et soit une application $i \mapsto A_i$ de I dans $\mathcal{P}(E)$ où E est un ensemble fini. On suppose que $i \neq j \Longrightarrow A_i \cap A_j = \emptyset$. Alors

$$\text{card}\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} \text{card}\,(A_i).$$

Voici maintenant une conséquence immédiate :

Théorème 2.2.5. *Soit $f : E \to F$ une application entre ensembles finis. Alors*

$$\text{card } E = \sum_{y \in F} \text{card}\left(f^{-1}(\{y\})\right).$$

Démonstration. On note que $E = \cup_{y \in F} f^{-1}(\{y\})$ (l'inclusion $\subset$ vient du fait que tout élément $e \in E$ est antécédent de son image donc $e \in f^{-1}(\{f(e)\})$; l'inclusion dans l'autre sens est évidente). Par ailleurs si $y, z \in F$ et $y \neq z$, $f^{-1}(\{y\}) \cap f^{-1}(\{z\})$ est vide (si x appartient à cet ensemble, $f(x)$ doit valoir à la fois y et z, ce qui est impossible). On peut donc conclure en disant que le cardinal de l'union disjointe vaut la somme des cardinaux. □

En voici une conséquence immédiate, utile pour les exercices :

Corollaire 2.2.6 (Principe des bergers)**.** *Soit $f : E \to F$ une application. On suppose que toutes les images réciproques $f^{-1}(\{y\})$, $y \in F$, ont le même nombre d'éléments q. Alors*

$$\text{card } E = q\,\text{card } F.$$

Exemple.
Pour compter des moutons, il suffit de compter les pattes et de diviser par 4. (Des applications plus significatives suivront !)

Le principe des bergers permet aussi d'établir l'expression du cardinal d'un produit cartésien :

Corollaire 2.2.7. *Si A et B sont des ensembles finis quelconques,*

$$\text{card } (A \times B) = \text{card } A \times \text{card } B.$$

Démonstration. On considère l'application $f : A \times B \to A$ définie par $f((x, y)) = x$. Pour tout $y \in B$, $f^{-1}(\{y\}) = \{(x, y);\ x \in A\}$ est clairement en bijection avec A (par $x \mapsto (x, y)$) donc a même cardinal que A. On en déduit que le cardinal de l'ensemble de départ vaut card A fois le cardinal de l'ensemble d'arrivée. □

2.3 Analyse combinatoire

Nous allons maintenant calculer le cardinal de plusieurs objets mathématiques (ensembles d'applications, de bijections, d'injections, des sous-ensembles d'un ensembles, etc...). Nous nous attacherons à mettre en avant les techniques standard, réutilisables dans les exercices.

2.3.1 Applications

Puissances. Fixons $a \in \mathbb{N}$. On définit a^n par récurrence sur n : $a^0 = 1$ et, pour tout $n \in \mathbb{N}$, $a^{n+1} := a.a^n$. On démontre (par récurrence !) les formules classiques : $a^{m+n} = a^m.a^n$, $(ab)^m = a^m b^m$ et $(a^m)^n = a^{mn}$.

Rappelons que $\mathcal{F}(E, F)$ désigne l'ensemble des applications de E dans F. On le note également F^E, ce qui se peut se justifier par l'analogie avec la formule suivante :

Théorème 2.3.1. *Soient E et F des ensembles finis. On a :* card $\mathcal{F}(E, F) = (\text{card } F)^{\text{card } E}$.

Démonstration. Elle se fait par récurrence sur $n := \text{card } E$. Nous noterons $q := \text{card } F$. Pour $n = 0$, il faut admettre que card $\mathcal{F}(\emptyset, F) = 1$. Si l'on trouve cette affirmation trop étrange (elle est pourtant rigoureusement exacte), on n'a qu'à l'admettre comme une pure convention et entamer la récurrence avec $n = 1$. Dans ce cas, E est un singleton : $E = \{x\}$ et on vérifie sans peine que l'application $\mathcal{F}(\{x\}, F) \to F$ qui à la fonction f associe la valeur $f(x)$ est une bijection.
Supposons l'affirmation vraie pour card $E = n$ et prouvons la pour card $E = n+1$. On écrit $E = E' \cup \{x\}$, où card $E' = n$ et où $x \notin E'$. L'hypothèse de récurrence nous dit que card $\mathcal{F}(E', F) = q^n$. Nous allons prouver, que card $\mathcal{F}(E, F) = q \,\text{card } \mathcal{F}(E', F)$. Considérons en effet l'application de restriction $f \mapsto f_{|F'}$ de $\mathcal{F}(E, F)$ dans $\mathcal{F}(E', F)$. L'image réciproque de $g \in \mathcal{F}(E', F)$ est formée des $f \in \mathcal{F}(E, F)$ qui prennent sur F' les mêmes valeurs que g et qui prennent en x une valeur arbitraire dans F. Il y a donc q telles applications f et le principe des bergers nous donne la conclusion. On a donc : card $\mathcal{F}(E, F) = q.q^n = q^{n+1}$, vue la définition par récurrence des puissances, ce qui achève la démonstration. □
Dans les dénombrements par récurrence, on essaie souvent de trouver une sous-structure de la famille à dénombrer qui soit de même nature. Dans la preuve précédente, on restreint les applications au sous ensemble F' par exemple et l'on remarque que ce sont toutes les applications de F' dans E.

2.3.2 Sous-ensembles

Etant donné un ensemble fini, on veut compter le nombre de ses sous-ensembles. **Un moyen efficace pour calculer le cardinal d'un ensemble est de montrer qu'il est en bijection avec un ensemble dont on connaît déjà le cardinal.** C'est ce que nous allons faire.

À tout sous-ensemble $F \subset E$, on associe sa *fonction caractéristique* 1_F : c'est l'application de E dans $\{0,1\}$ définie par :

$$\forall x \in E\ ,\ 1_F(x) := \begin{cases} 1 \text{ si } x \in F, \\ 0 \text{ si } x \notin F. \end{cases}$$

Théorème 2.3.2. *L'application $F \mapsto 1_F$ est une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E,\{0,1\})$.*

Démonstration. Notons χ l'application $\mathcal{P}(E) \to \mathcal{F}(E,\{0,1\})$ définie par $F \mapsto 1_F$. Nous pourrions vérifier directement que c'est une bijection, ce qui demande de montrer que tout élément de l'espace d'arrivée a une unique antécédent. Pour ce problème précis, comme l'application réciproque n'est pas difficile à deviner, nous allons d'abord la définir par une formule directe et ensuite vérifier que c'est bien la réciproque.

Considérons l'application Supp : $\mathcal{F}(E,\{0,1\}) \to \mathcal{P}(E)$, qui à toute application $\phi : E \to \{0,1\}$ associe son *support* $\mathrm{Supp}(\phi) := \phi^{-1}(\{1\}) = \{x \in E,\ \phi(x) = 1\}$, qui est une partie de E. On vérifie alors que

$$\chi \circ \mathrm{Supp} = \mathrm{Id}_{\mathcal{F}(E,\{0,1\})} \quad \text{et} \quad \mathrm{Supp} \circ \chi = \mathrm{Id}_{\mathcal{P}(E)}.$$

Nous laissons le lecteur vérifier ces relations simples (la première signifie que la fonction caractéristique du support de ϕ n'est autre que ϕ ; la seconde que le support de la fonction caractéristique de F n'est autre que F). Les applications $F \mapsto \chi_F$ et $\phi \mapsto \mathrm{Supp}(\phi)$ sont donc réciproques l'une de l'autre ; F est bijective (c'est ce que dit le théorème 2.1.1). □

Corollaire 2.3.3. *Soit E un ensemble fini. On a :* $\mathrm{card}\ \mathcal{P}(E) = 2^{\mathrm{card}\ E}$.

Remarque : L'intérêt de l'argument qui précède, en plus de montrer que $\mathcal{F}(E,\{0,1\})$ et $\mathcal{P}(E)$ ont le même cardinal, est de l'expliquer par une bijection simple. Remarquons que lorsque $\mathrm{card}\ A = \mathrm{card}\ B = n$, par définition il existe deux bijections $\phi : [\![1,n]\!] \to A$ et $\psi : [\![1,n]\!] \to B$. Alors $\psi \circ \phi^{-1}$ est une bijection de A dans B. Nous savons qu'elle existe, mais nous ne savons pas forcément la décrire et elle est peut-être compliquée. Un réflexe naturel en combinatoire est, lorsque l'on a montré par des méthodes séparées que deux ensembles ont le même cardinal, de se demander s'il existe une raison simple à cette égalité, c'est-à-dire s'il existe une bijection facile à décrire entre les deux ensembles.

2.3.3 Arrangements, injections

Soient E et F deux ensembles finis ayant respectivement m et n éléments. Nous noterons $I(E,F)$ l'ensemble des applications injectives de E dans F. Si $m > n$, il n'y en a aucune et $I(E,F) = \emptyset$. Nous allons calculer $\mathrm{card}\ I(E,F)$ lorsque $m \leq n$.

Remarquons d'abord que si $\mathrm{card}\ E = \mathrm{card}\ E'$ et $\mathrm{card}\ F = \mathrm{card}\ F'$, alors $\mathrm{card}\ I(E,F) = \mathrm{card}\ I(E',F')$. Détaillons l'argument (nous l'utiliserons sans répéter la preuve dans d'autres situations) : considérons des bijections $\phi : E \to E'$ et $\psi : F \to F'$. Si $f : E \to F$ est une injection, alors l'application $\psi \circ f \circ \phi^{-1} : E' \to F'$ est encore une injection (voir l'exercice 25). On peut donc définir une application $K : I(E,F) \to I(E',F')$ par $K(f) := \psi \circ f \circ \phi^{-1}$. Le

même argument, en inversant les rôles, donne une application $L : I(E', F') \to I(E, F)$ définie par $K(g) := \psi^{-1} \circ g \circ \phi$. Un calcul immédiat montre que $L \circ K = \mathrm{Id}_{I(E,F)}$ et $K \circ L = \mathrm{Id}_{I(E',F')}$. Donc K et L sont des bijections réciproques et on a établi $\mathrm{card}\, I(E, F) = \mathrm{card}\, I(E', F')$.

Ainsi $\mathrm{card}\, I(E, F)$ ne dépend que de $m = \mathrm{card}\, E$ et $n = \mathrm{card}\, F$. On le note A_n^m (donc $A_n^m = 0$ lorsque $m > n$). En particulier, on peut aussi bien supposer que $E = [\![1, m]\!]$. Dans ce cas, se donner une application $f : [\![1, m]\!] \to F$ revient à se donner une suite $(f(1), \ldots, f(m)) \in F^m$. De plus une application f injective correspond à une suite $(f(1), \ldots, f(m))$ dont tous les éléments sont distincts.

On appelle *arrangement de m objets pris parmi les n éléments de F* toute suite $(y_1, \ldots, y_m)$ de m éléments distincts de F. Ainsi compter les injections revient à compter les arrangements.

Lemme 2.3.4. *Si $0 \leq m \leq n-1$, on a : $A_n^{m+1} = (n-m)A_n^m$.*

Démonstration. À toute suite $(y_1, \ldots, y_{m+1})$ de $(m+1)$ éléments distincts de F, associons la suite $(y_1, \ldots, y_m)$ de m éléments distincts de F. On obtient ainsi une application ϕ de $I([\![1, m+1]\!], F)$ dans $I([\![1, m]\!], F)$. L'image réciproque de $(y_1, \ldots, y_m)$ par ϕ est formée de toutes les suites $(y_1, \ldots, y_m, y)$ telles que $y \in F \setminus \{y_1, \ldots, y_m\}$: cette image réciproque a donc $(n-m)$ éléments. D'après le principe des bergers, $\mathrm{card}\, I([\![1, m+1]\!], F) = (n-m)\,\mathrm{card}\, I([\![1, m]\!], F)$. □

Théorème 2.3.5. *Le nombre d'injections d'un ensemble à m éléments dans un ensemble à n éléments vaut*

$$A_n^m = \begin{cases} 0 & \text{si} \quad m > n \\ \dfrac{n!}{(n-m)!} = \displaystyle\prod_{i=0}^{m-1} (n-i) & \text{si} \quad m \leq n \end{cases}$$

Il est aussi égal au nombre d'arrangements de m objets pris parmi n.

Démonstration. Il nous reste seulement à démontrer la formule pour A_n^m lorsque $m \leq n$. On le fait par récurrence sur m. Pour $m = 0$, l'unique application de $\emptyset$ dans F est injective et l'on trouve $A_n^0 = 1 = \dfrac{n!}{n!}$, ce qui est correct. Si l'on trouve l'argument trop bizarre, on admet cette valeur comme une convention et l'on initialise la récurrence à $m := 1$. Dans ce cas, E est un singleton et les n applications de E dans F sont injectives : on a bien $A_n^1 = \dfrac{n!}{(n-1)!} = n$. On peut également dire que les arrangements de 1 objet pris parmi n sont ici les n suites (y) de 1 élément de F.
Supposons maintenant que $A_n^m = \dfrac{n!}{(n-m)!}$ pour un certain $m \in [\![0, n-1]\!]$. En combinant le lemme et l'hypothèse de récurrence, on trouve :

$$A_n^{m+1} = (n-m)A_n^m = (n-m)\frac{n!}{(n-m)!} = \frac{n!}{\big(n-(m+1)\big)!},$$

d'où la première égalité. L'égalité $\dfrac{n!}{(n-m)!} = \displaystyle\prod_{i=0}^{m-1} (n-i)$ est immédiate. □

Lorsque $m = n$, toute application de E dans F est injective si et seulement si elle est bijective. Donc A_n^n représente le nombre de bijections entre deux ensembles de cardinal n. Le nombre A_n^n représente aussi le nombre d'arrangements $(y_1, \ldots, y_n)$ formés des n éléments de F, chacun étant (bien entendu) présent une fois et une seule. Une telle suite est appelée *permutation* de F. Une définition essentiellement équivalente est celle-ci : une permutation de F est une bijection de F dans lui-même.

Théorème 2.3.6. *Le nombre de bijections entre deux ensembles à n éléments est $n!$.*
Le nombre de permutations d'un ensemble à n éléments est $n!$.

Démonstration. C'est $A_n^n = \dfrac{n!}{(n-n)!} = \dfrac{n!}{0!} = n!$. □

Exercice 28. Décrire tous les arrangements de $1, 2, 3$ objets pris parmi les 4 éléments $\{1, 2, 3, 4\}$.

Exercice 29. Décrire toutes les permutations de $F := \{1, 2, 3\}$.

2.3.4 Combinaisons

Soit E un ensemble à n éléments. Lorsque $0 \leq m \leq n$, on appelle *combinaison de m objets pris parmi les n éléments de E* un sous-ensemble $\{y_1, \ldots, y_m\}$ formé de m éléments distincts de E : ce n'est donc rien d'autre qu'un sous-ensemble à m éléments de n. La différence entre une combinaison et un arrangement, c'est que l'ordre importe dans un arrangement mais pas dans une combinaison. Le nombre de ces combinaisons ne dépend évidemment que de m et de n. On le note traditionnellement C_n^m et, de manière plus moderne (influencée par l'univers anglo-saxon !) $\binom{n}{m}$, ce qui se lit : "choix de m parmi n". Les $C_n^m = \binom{n}{m}$ sont appelés *coefficients binomiaux* pour des raisons qui apparaitront à la section 2.4.3. On convient que $\binom{n}{m} = 0$ lorsque $m > n$. (Pourquoi ?)

Exercice 30. Décrire toutes les combinaisons de 1, 2, 3 objets pris parmi les 4 éléments $\{1, 2, 3, 4\}$.

Théorème 2.3.7. *Lorsque $0 \leq m \leq n$, le nombre de combinaisons de m objets pris parmi n est donné par la formule :*

$$C_n^m = \binom{n}{m} = \frac{n!}{m!\,(n-m)!}.$$

Démonstration. À chaque arrangement $(y_1, \ldots, y_m)$ dans E, associons l'ensemble $\{y_1, \ldots, y_m\}$ sous-jacent, obtenu en oubliant l'ordre. Les arrangements ayant pour image une combinaison $\{y_1, \ldots, y_m\}$ donnée sont les $m!$ permutations de $(y_1, \ldots, y_m)$. D'après le principe des bergers, on a donc $A_n^m = m!\, C_n^m$, d'où la conclusion. □

Corollaire 2.3.8. *Le nombre d'applications strictement croissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est $\binom{n}{m}$.*

Démonstration. L'idée est qu'une application strictement croissante f de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est totalement déterminée par son image $\{y_1, \ldots, y_m\} \subset [\![1, n]\!]$: le plus petit élément est $f(1)$, le suivant est $f(2)$, etc. Nous laissons le lecteur formuler ceci en termes de bijections. □

2.4 Propriétés des coefficients binomiaux

2.4.1 Variations

Nous décrivons les variations de $m \mapsto \binom{n}{m}$ pour n fixé. On ne s'intéresse qu'à $0 \leq m \leq n$ car sinon les coefficients sont nuls.

Proposition 2.4.1. *Pour $0 \leq m \leq n$, on a :* $\binom{n}{m} = \binom{n}{n-m}$.

Démonstration. La formule est immédiate par calcul sur l'expression $\binom{n}{m} = \dfrac{n!}{m!\,(n-m)!}$.

On peut également la justifier en remarquant que, si card $E = n$, l'application $F \mapsto E \setminus F$ (passage au complémentaire dans E) est une bijection de l'ensemble des parties de E à m éléments sur l'ensemble des parties de E à $(n-m)$ éléments. □

Proposition 2.4.2. *Si n est pair, l'application $m \mapsto \binom{n}{m}$ croît strictement de $m = 0$ à $m = n/2$ (où elle prend sa valeur maximum) puis décroît strictement de $m = n/2$ à $m = n$*

Si n est impair, cette suite croît strictement de $m = 0$ à $m = (n-1)/2$, prend la même valeur (son maximum) en $m = (n-1)/2$ et $m = (n+1)/2$, puis décroît strictement de $m = (n+1)/2$ à $m = n$.

Démonstration. Soient m, n tels que $0 \leq m \leq n-1$. On obtient après simplification la formule :

$$\frac{\binom{n}{m+1}}{\binom{n}{m}} = \frac{n-m}{m+1}.$$

On déduit que $\binom{n}{m+1} > \binom{n}{m}$ si, et seulement si, $2m \leq n$. On en tire les variations de la suite des $\binom{n}{m}$ à n fixé. □

2.4.2 Le triangle de Pascal

Théorème 2.4.3 (Formule de Pascal)**.** *Pour tous $m, n \in \mathbb{N}$ on a :*

$$\binom{n+1}{m+1} = \binom{n}{m+1} + \binom{n}{m}.$$

Démonstration. Si $m > n$, les deux membres de l'égalité sont nuls. Si $m = n$, $\binom{n+1}{m+1} = \binom{n}{m} = 1$ et $\binom{n}{m+1} = 0$, et les deux membres de l'égalité sont égaux à 1. On peut donc supposer que $0 \leq m < n$. Nous disposons dans ce cas de deux preuves tout à fait différentes. La preuve calculatoire vient immédiatement à l'esprit :

$$\begin{aligned}
\binom{n}{m+1} + \binom{n}{m} &= \frac{n!}{(m+1)!\,\big(n-(m+1)\big)!} + \frac{n!}{m!\,(n-m)!} \\
&= (n-m)\frac{n!}{(m+1)!\,(n-m)!} + (m+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= (n+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= \frac{(n+1)!}{(m+1)!\,(n-m)!} \\
&= \binom{n+1}{m+1}.
\end{aligned}$$

La preuve combinatoire revient à montrer que les deux nombres comptent la même chose. Considérons un ensemble E à n éléments soit $E' := E \cup \{x\}$ avec $x \notin E$. Donc E' a $(n+1)$ éléments. L'entier $\binom{n+1}{m+1}$ est le nombre de parties de E' qui ont $(m+1)$ éléments. Il y en a de deux types :

(1) Les parties à $(m+1)$ éléments de E : il y en a $\binom{n}{m+1}$.

(2) Les $F \cup \{x\}$, où F est une partie à m éléments de E : il y en a $\binom{n}{m}$.

Au total, on a bien $\left(\binom{n}{m+1} + \binom{n}{m}\right)$ parties à $(m+1)$ éléments de E'. □

On peut calculer les coefficients binomiaux à l'aide du *triangle de Pascal* :

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

La règle de formation est la suivante : les côtés du triangle sont formés de 1 ; chaque coefficient du tableau est la somme de ceux qui lui sont supérieurs juste à gauche et juste à droite. Sur la n^{e} ligne on trouve alors de gauche à droite les $\binom{n}{m}$ pour $m = 0, 1, \ldots, n$.

La formule de Pascal permet également un calcul "récursif" des coefficients binomiaux par l'algorithme suivant :

```
Pasc(n,m)
si m = 0 alors rendre 1 sinon si n = 0 alors rendre 0
sinon rendre Pasc(n-1,m) + Pasc(n-1,m-1) ;;
```

Le lecteur intéressé pourra rechercher la "complexité" de cet algorithme ; par exemple, combien d'additions requiert-il ? Et dans quelle mesure les calculs sont-ils redondants ?

Il est très facile d'obtenir le triangle de Pascal avec un tableur : On remplit la première colonne avec des 1 (par copier-coller bien entendu !). Ensuite on remplit les cases vides de la première ligne avec des 0. Enfin dans toutes les cases restantes, on entre la même formule qui dit que la valeur de la case est la somme de la valeur de la case immédiatement au-dessus et de la case au-dessus à gauche. Le résultat apparaît sous une forme moins symétrique :

$$\begin{array}{ccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 0 & 0 & 0 & 0 \\
1 & 3 & 3 & 1 & 0 & 0 & 0 \\
1 & 4 & 6 & 4 & 1 & 0 & 0 \\
1 & 5 & 10 & 10 & 5 & 1 & 0 \\
1 & 6 & 15 & 20 & 15 & 6 & 1
\end{array}$$

2.4.3 La formule du binôme de Newton

Théorème 2.4.4 (Formule du binôme de Newton)**.** *Soient a et b deux nombres complexes. On a alors, pour tout $n \in \mathbb{N}$:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. Elle se fait par récurrence sur n. Pour $n = 0$, il s'agit de vérifier que $(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$, autrement dit, que $1 = \binom{0}{0} a^0 b^0$, ce qui est bien vrai. Supposons la formule vraie au rang n. On calcule alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n-j+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \left(\binom{n}{j-1} + \binom{n}{j} \right) a^j b^{n-j+1} + b^{n+1} \\
&= \sum_{j=1}^{n+1} \binom{n+1}{j} a^j b^{n-j+1} + \binom{n}{0} a^0 b^{n-0+1} \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j}.
\end{aligned}$$

□

Un peu d'algèbre combinatoire. Si l'on développe $(a+b)^n = (a+b)\cdots(a+b)$ (n facteurs), on voit apparaitre des termes de la forme $a^k b^{n-k}$. Chacun de ces termes apparait autant de fois qu'il y a de choix des k facteurs $(a+b)$ dans lesquels on prend a plutôt que b, donc, au total $\binom{n}{k}$ fois : c'est une autre preuve de la formule de Newton. Notons que les seules propriétés utilisées sont la commutativité et l'associativité de l'addition et de la multiplication, ainsi que la distributivité.

Exemple.
Une application directe de la formule du binôme donne

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k}.$$

On peut aussi interpréter (et démontrer) cette formule de manière combinatoire : un ensemble E de cardinal n a au total 2^n parties, dont $\binom{n}{0}$ à 0 éléments, $\binom{n}{1}$ à 1 élément, $\binom{n}{2}$ à 2 éléments, etc.

Exercice 31. Développer les expressions $(1-x)^3$, $(1+x)^6$ et $(1+x)^7$.

2.4.4 Et bien d'autres formules...

Les coefficients binomiaux satisfont beaucoup de relations, ce qui explique l'attention qui leur a été portée. Nous donnons un exemple parmi tant d'autres, ainsi qu'une preuve combinatoire :

$$\sum_{p=0}^{q} \binom{m}{p} \binom{n}{q-p} = \binom{m+n}{q}.$$

Soient E et F deux ensembles disjoints ayant respectivement m et n éléments. L'ensemble $E \cup F$ a $(m+n)$ éléments, donc $\binom{m+n}{q}$ sous-ensembles à q éléments. Chacun de ces sous-ensembles est de la forme $E' \cup F'$, où $E' \subset E$ a p éléments (pour un p tel que $0 \leq p \leq q$) et où $F' \subset F$ a $(q-p)$ éléments. Pour chaque p, il y a $\binom{m}{p}\binom{n}{q-p}$ tels ensembles $E' \cup F'$, et leur nombre total est bien $\sum_{p=0}^{q} \binom{m}{p}\binom{n}{q-p}$.

Une preuve de nature algébrique est proposée à l'exercice 58 en fin de chapitre. L'exercice 52 présente une autre formule remarquable.

2.5 Compléments

2.5.1 Nombre de surjections

Notons $n := \text{card } E$ et $p := \text{card } F$. Nous allons compter le nombre $S(n,p)$ d'applications surjectives de E dans F. Naturellement, on peut tout aussi bien supposer que $F = [\![1,p]\!]$, ce que nous ferons. Pour tout $i \in F$, soit $\mathcal{F}_i := \{f \in \mathcal{F}(E,F) \mid i \notin \text{Im} f\}$. Par définition, l'ensemble des surjections est égal à $\mathcal{F}(E,F) \setminus \bigcup_{i \in F} \mathcal{F}_i$, de sorte que $S(n,p) = p^n - \text{card} \bigcup_{i \in F} \mathcal{F}_i$. Nous allons calculer le cardinal de $\bigcup_{i \in F} \mathcal{F}_i$ à l'aide de la formule du crible :

$$\text{card} \bigcup_{i \in F} \mathcal{F}_i = \text{card} \bigcup_{i=1}^{p} \mathcal{F}_i = \sum_{k=1}^{p} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq p} \text{card}\,(\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}).$$

L'ensemble $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des applications $f : E \to F$ telles que $i_1, \ldots, i_k \notin \text{Im} f$, autrement dit, des applications de E dans $F \setminus \{i_1, \ldots, i_k\}$. Comme ce dernier ensemble a $p-k$ éléments, on déduit du théorème : $\text{card}\,(\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}) = (p-k)^n$. Anticipant sur la section 2.3.3 et notant $\binom{p}{k}$ le nombre de parties à k éléments $\{i_1, \ldots, i_k\} \subset F$:

$$S(n,p) = p^n - \sum_{k=1}^{p} (-1)^{k-1} \binom{p}{k} (p-k)^n = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.$$

2.5.2 Combinatoire des ensembles infinis, dénombrabilité

Il est possible de faire de la combinatoire sur les ensembles infinis, en s'inspirant du cas fini. On dira que deux ensembles E et F ont "autant d'éléments" s'il existe une bijection de E dans F. Cette définition correspond bien à ce que nous avons fait pour les ensembles finis, mais elle nous réserve des surprises dans le cas infini. Ainsi, l'application $f : \mathbb{N} \to \mathbb{N}^*$ définie par $n \mapsto n+1$ est une bijection, donc $\mathbb{N}^*$ a autant d'éléments que $\mathbb{N}$ alors même qu'on lui a enlevé l'élement 0 (au fond ce n'est pas si choquant, l'infini moins un reste infini...). On peut aussi voir que $\mathbb{N}$ a autant d'éléments que l'ensemble $2\mathbb{N}$ des entiers pairs (exercice 32) et même que l'ensemble $\mathbb{N} \times \mathbb{N}$ (exercice 33).

Poursuivant l'analogie avec le cas fini (trois premier points du théorème 2.2.1), on a envie de dire que "E n'a pas (strictement) plus d'éléments que F" signifie pour des ensembles généraux (finis ou infinis) qu'il existe une injection de E dans F, et que "E n'a pas (strictement) moins d'éléments que F" signifie qu'il existe une surjection de E dans F. Il n'est pas évident que ces notions soient cohérentes : on voudrait que "E n'a pas plus d'éléments que F" entraine que "F n'a pas moins d'éléments que E". On voudrait aussi que si E n'a ni plus, ni moins d'éléments que F ils aient le même nombre d'éléments!! Ce n'est pas évident pour des ensembles infinis, mais c'est vrai comme l'affirme le résultat suivant (que nous admettrons)

Proposition 3. *On a les propriétés suivantes*

(1) S'il existe une injection $E \to F$, il existe une surjection $F \to E$.

(2) S'il existe une surjection $E \to F$, il existe une injection $F \to E$.

(3) S'il existe une injection $E \to F$ et une surjection $E \to F$, il existe une bijection $E \to F$.

Cette propriété n'est pas très difficile à montrer en utilisant *l'axiome du choix*. Cet axiome (qu'on ne peut pas démontrer à partir des propriétés déjà énoncées sur les ensembles) nous dit que si on a une application de $f : E \to \mathcal{P}(F)$ telle que, $\forall x \in E,\ f(x) \neq \emptyset$, il existe une application $g : E \to F$ telle que, $\forall x \in E, g(x) \in f(x)$. On le traduit en général par la phrase (beaucoup moins précise) "Si l'on a une famille d'ensembles non vides, on

peut choisir un élément de chaque ensemble". Aussi anodin que puisse paraître cet axiome, c'est en fait un outil très puissant (et dangereux à manier sans précautions). On peut par exemple en déduire qu'on peut découper une pomme en un nombre fini de morceaux et qu'en recollant ces morceaux, on obtienne la lune ! (Bien sûr, ces morceaux auront une "forme" très très particulière, et difficilement imaginable.)

Retenons simplement qu'il existe une bonne notion de cardinal des ensembles infinis et revenons à l'exemple de l'ensemble $\mathbb{N}$. On dira qu'un ensemble E est *dénombrable* s'il a autant d'éléments que $\mathbb{N}$ (s'il est en bijection avec $\mathbb{N}$, ce qui revient à la possibilité de l'écrire $E = \{e_0, e_1, e_2, \ldots\}$). Il est facile de voir que $\mathbb{N}$ est le plus petit des ensembles infinis : tout ensemble infini contient au moins autant d'éléments que $\mathbb{N}$; c'est très facile : si E est infini il n'est pas vide, donc il contient un élément e_1. Il n'est pas non plus de cardinal 1, donc il contient un élément e_2 différent de e_1, il n'est pas de cardinal 3, donc il contient un $e_3 \notin \{e_1, e_2\}$. En répétant le procédé, on construit une injection de $\mathbb{N} \to E$ telle que $n \mapsto e_n$.

Il y a de nombreux ensembles dénombrables qu'on rencontre naturellement . Nous avons évoqué l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers. On voit plus facilement que $\mathbb{Z}$ est dénombrable (une manière de l'énumérer est d'écrire $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$). L'ensemble $\mathbb{Q}$ des nombres rationnels est lui aussi dénombrable. Ceci peut sembler très curieux : il semble pourtant qu'il y a beaucoup plus de points dans $\mathbb{Q}$ que dans $\mathbb{N}$. Et pourtant, il n'en est rien ! En effet l'application $i : \mathbb{N} \to \mathbb{Q}$, $n \mapsto n$ est injective. Par ailleurs, comme $\mathbb{N}^*$ et $\mathbb{Z}$ sont en bijection avec $\mathbb{N}$, $\mathbb{N}^* \times \mathbb{Z}$ est en bijection avec $\mathbb{N} \times \mathbb{N}$ donc est aussi dénombrable. Or l'application $\mathbb{N}^* \times \mathbb{Z} \to \mathbb{Q}$, $(p, q) \mapsto q/p$ est clairement surjective. Tout ceci donne une surjection de $\mathbb{N}$ sur $\mathbb{Q}$. La proposition précédente nous assure qu'il existe une bijection entre $\mathbb{N}$ et $\mathbb{Q}$. Enfin mentionons qu'une union finie ou dénombrable d'ensembles dénombrables est dénombrable et qu'un produit fini d'ensembles dénombrables est dénombrable.

Tous les ensembles ne sont pas dénombrables loin de là ! En effet, **il n'y a jamais de surjection de E dans $\mathcal{P}(E)$**. L'ensemble des parties d'un ensemble a toujours plus d'éléments (beaucoup plus !) que l'ensemble lui même. Nous le verrons à l'exercice 36. Par conséquent $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable. L'ensemble $\mathbb{R}$ ou $[0, 1] = \{x \in \mathbb{R};\ 0 \leq x \leq 1\}$ non plus. En fait on peut voir que $\mathbb{R}$ a autant d'élements que $\mathcal{P}(\mathbb{N})$.

Exercices

Exercice 32. Les applications suivantes sont-elles injectives, surjectives, bijectives ?

(1) $c : \mathbb{R} \to \mathbb{R}$ telle que $\forall x, c(x) = x^2$.

(2) $d : [1, 2] \to [0, 4]$ telle que $\forall x, d(x) = x^2$.

(3) $f : \mathbb{N} \to \mathbb{N}$ telle que $\forall n$, $f(n) = n + 1$.

(4) $g : \mathbb{N} \to \mathbb{N}^*$ telle que $\forall n$, $g(n) = n + 1$.

(5) On note $2\mathbb{N}$ l'ensemble des entiers naturels pairs. On définit $h : \mathbb{N} \to 2\mathbb{N}$ par $n \mapsto 2n$ pour tout $n \in \mathbb{N}$.

Exercice 33. (*) Démontrer que l'application $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ qui au couple (n, p) associe $f(n, p) = 2^n(2p + 1)$ est une bijection.

Exercice 34. (*) Soit E un ensemble non vide, et $A \subset E$. On considère l'application $\phi : \mathcal{P}(E) \to \mathcal{P}(E)$ qui à $B \subset E$ associe $\phi(B) = B \cap A$.

(1) Montrez que ϕ est injective si et seulement si $A = E$.

(2) Montrez que ϕ est surjective si et seulement si $A = E$.

Exercice 35. (*) Soit E un ensemble non vide, et $A \subset E$. On considère l'application $\phi : \mathcal{P}(E) \to \mathcal{P}(E)$ qui à $B \subset E$ associe $\phi(B) = B \cup A$.

(1) Montrez que ϕ est injective si et seulement si $A = \emptyset$.

(2) Montrez que ϕ est surjective si et seulement si $A = \emptyset$.

Exercice 36. (**) Dans cet exercice, on montre qu'il ne peut pas avoir d'application surjective de E dans $\mathcal{P}(E)$.

Soit $f : E \to \mathcal{P}(E)$. On considère $A = \{x \in E, x \notin f(x)\}$. Montrez que s'il existe $y \in E$ tel que $A = f(y)$, alors,

(1) $y \in A \implies y \notin A$.

(2) $y \notin A \implies y \in A$.

Conclure.

Exercice 37. (**) [Décomposition d'une application] On considère une application $f : E \to F$.

(1) Montrez que la relation $x \sim y \iff f(x) = f(y)$ est une relation d'équivalence.

(2) On considère $E_1 = E/\sim$ l'ensemble quotient de E par cette relation. On définit une application $b : E_1 \to f(E)$ de la façon suivante : pour $a \in E_1$, on choisit $x \in A$ et on pose $g(a) = f(x)$. Montrez que cela définit bien une application.

(3) Montrez que l'application g de la question précédente est une bijection.

(4) On définit $s : E \to E_1$ par $s(x) = \dot{x}$, où $\dot{x}$ est la classe de x. Montrez que c'est une surjection.

(5) En déduire que toute application se décompose en $i \circ b \circ s$ où i est une injection, b une une bijection et s une surjection.

Exercice 38. Combien de poignées de main échangent n personnes qui se rencontrent ? (on suppose que chacune d'entre elles serre la main de toutes les autres)

Exercice 39. Combien y a-t-il d'applications possibles de $\{1, 2, 3\}$ dans lui même ? Décrire toutes les bijections.

Exercice 40. Démontrer sans calcul qu'il y a autant d'applications croissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$ que d'applications décroissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$.

Exercice 41. Avec un jeu de 32 cartes, combien y a-t-il de mains (c'est-à-dire d'ensembles) de 5 cartes contenant :

(1) un carré d'as ?

(2) exactement deux rois ?

(3) au moins deux rois ?

(4) une suite longue (5 cartes consécutives dans la même famille) ?

(5) un full (trois cartes de la même hauteur et deux autres cartes de même hauteur) ?

Exercice 42. Combien d'entiers de $[\![100, 999]\!]$ ont au moins un chiffre 7 en écriture décimale ?

Exercice 43. Soit $n \geq 1$. Calculer le nombre d'applications f de $\{1, \dots, 2n\}$ dans lui-même qui vérifient que pour tout k, les nombres k et $f(k)$ ont la même parité.

Exercice 44. (**) Interpréter les formules $a^{m+n} = a^m.a^n$, $(ab)^m = a^m b^m$ et $(a^m)^n = a^{mn}$ à l'aide de bijections.

Exercice 45. Un carré latin de taille n est un tableau de n lignes et n colonnes, rempli par des nombres de 1 à n et respectant la règle suivante : chaque nombre $k \in \{1, \dots, n\}$ apparaît une fois et une seule dans chaque ligne et dans chaque colonne. Dénombrer les carrés latins de taille 2, puis de taille 3.

Remarques : Un sudoku est un carré latin de taille 9 qui vérifie une règle supplémentaire. Leur dénombrement est une tâche autrement difficile. Il y en a 6709037520210729360. Par ailleurs, on ne connaît pas à ce jour de formule générale explicite donnant le nombre de carrés latins de taille n.

Exercice 46. (*) Construire explicitement une bijection entre $[\![1, a]\!] \times [\![1, b]\!]$ et $[\![1, ab]\!]$.

Exercice 47. (*) Soit $n \geq 1$ et E un ensemble de cardinal n. On notera $\mathcal{P}_{\text{pair}}(E)$ l'ensemble des parties de E de cardinal pair et $\mathcal{P}_{\text{impair}}(E)$ l'ensemble de celles de cardinal impair. Le but de cet exercice est de démontrer sans calcul que $\text{card}\big(\mathcal{P}_{\text{pair}}(E)\big) = \text{card}\big(\mathcal{P}_{\text{impair}}(E)\big)$.

(1) Vérifiez-le lorsque $E = \{1, 2\}$ puis lorsque $E = \{1, 2, 3\}$ (on décrira $\mathcal{P}(E)$).

(2) On considère l'application $F : \mathcal{P}(E) \to \mathcal{P}(E)$ définie par $F(A) = A^c$. Montrer que $F \circ F = \text{Id}$. En déduire que F est une bijection de $\mathcal{P}(E)$.

(3) Montrer l'application $\widetilde{F} : \mathcal{P}_{\text{pair}}(E) \to F(\mathcal{P}_{\text{pair}}(E))$ définie par $\widetilde{F}(A) = F(A)$ (c'est une restriction de F) est une bijection. En déduire que si n est impair, $\widetilde{F}$ est une bijection entre $\mathcal{P}_{\text{pair}}(E)$ et $\mathcal{P}_{\text{impair}}(E)$ et conclure.

(4) Soit $e \in E$ un élément fixé. On considère maintenant l'application $G : \mathcal{P}(E) \to \mathcal{P}(E)$ définie par :

$$G(A) = A \cup \{e\} \quad \text{si } e \notin A,$$
$$G(A) = A \setminus \{e\} \quad \text{si } e \in A.$$

Montrer que $G \circ G = \text{Id}$. Utiliser G pour construire une bijection entre $\mathcal{P}_{\text{pair}}(E)$ et $\mathcal{P}_{\text{impair}}(E)$.

Exercice 48. (*) Soit E un ensemble à n éléments. Calculer le cardinal de

$$\big\{(X, Y) \in \mathcal{P}(E) \times \mathcal{P}(E);\ X \subset Y\big\}.$$

Indication : on pourra commencer par calculer pour un sous-ensemble Y fixé de E, le cardinal de $\big\{X \in \mathcal{P}(E);\ X \subset Y\big\}$.

Exercice 49. (*) Soit $E \subset \mathbb{C}^*$ un ensemble à n éléments et soit $p \in \mathbb{N}^*$. Combien y a-t-il de nombres complexes tels que $z^p \in E$?

Exercice 50. (**) Dans un dé "polyédrique" (nombre quelconque de faces ayant chacune un nombre quelconque de côtés), il y a deux faces qui ont le même nombre de côtés.

Exercice 51. (**) Le but de cet exercice est de montrer que le nombre d'applications croissantes de $[\![1,m]\!]$ dans $[\![1,n]\!]$ est $\binom{m+n-1}{m}$.

(1) Soit $f : [\![1,m]\!] \to [\![1,n]\!]$ une application croissante. Montrez que pour tout $k \in [\![1,m]\!]$, $f(k)+k-1 \leqq m+n-1$. En déduire que l'application $\widetilde{f} : [\![1,m]\!] \to [\![1,m+n-1]\!]$ telle que pour tout k, $\widetilde{f}(k) = f(k)+k-1$ est bien définie et est strictement croissante.

(2) Utiliser la question précédente pour construire une bijection entre l'ensemble des fonctions croissantes de $[\![1,m]\!]$ dans $[\![1,n]\!]$ d'une part, et l'ensemble des fonctions strictement croissantes de $[\![1,m]\!]$ dans $[\![1,m+n-1]\!]$.

(3) Conclure.

Exercice 52. (*) Soient $q \geq p \geq 0$ des entiers.

1. Démontrer par récurrence sur q la formule : $\sum_{n=p}^{q} \binom{n}{p} = \binom{q+1}{p+1}$.
2. Expliciter la formule ci-dessus pour $p = 0, 1, 2$. En déduire une expression courte de $\sum_{n=1}^{q} n^2$.

Exercice 53. (*) Calculer $\sum_{n=1}^{q} n^3$.

Exercice 54. (*) Soient $n, p \in \mathbb{N}^*$. Montrer par récurrence sur n que le nombres de n-uplets d'entiers naturels $(x_1, \ldots, x_n) \in \mathbb{N}^n$ tels que $x_1 + \cdots + x_n = p$ est égal à $\binom{p+n-1}{p}$.

Indication : pour l'hérédité on pourra isoler une variable. Par ailleurs on aura besoin de la formule démontrée à la première question de l'exercice 52.

Exercice 55. (*) Calculer $\sum_{X \in \mathcal{P}([\![1,n]\!])} \mathrm{card}(X)$.

Exercice 56. (*) Calculer $\sum_{(X,Y) \in \mathcal{P}([\![1,n]\!]) \times \mathcal{P}([\![1,n]\!])} \mathrm{card}(X \cap Y)$.

Indication : on pourra utiliser la relation $\mathrm{card}\,(X) = \sum_{i=1}^{n} \mathbf{1}_X(i)$ pour $X \subset [\![1,n]\!]$).

Exercice 57. Soit $n \geq 1$.

1. En calculant de deux manières les quantités $(1+1)^n$ et $(1-1)^n$ montrer que

$$\sum_{k \in P_n} \binom{n}{k} = \sum_{k \in I_n} \binom{n}{k} = 2^{n-1},$$

où P_n est l'ensemble des entiers pairs inférieurs ou égaux à n et I_n est celui des entiers impairs inférieurs ou égaux à n (par exemple si n est pair $\sum_{k \in P_n} \binom{n}{k} = \binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{n}$).

2. En déduire le résultat de l'exercice 47.

Exercice 58. Calculer de deux manières le terme en x^q dans $(1+x)^m(1+x)^n = (1+x)^{m+n}$, et en déduire l'égalité :

$$\sum_{p=0}^{q} \binom{m}{p}\binom{n}{q-p} = \binom{m+n}{q}.$$

Exercice 59. (**) Soit $f : F \to F$ une application bijective (donc une permutation). On dit que c'est un *dérangement* de F si : $\forall y \in F,\ f(y) \neq y$.

(1) Décrire tous les dérangements de $\{1, 2, 3, 4\}$.

(2) Nous prendrons $F := \{1, \ldots, n\}$. Nous noterons S_n l'ensemble de toutes les permutations de F et D_n l'ensemble de tous les dérangements de F et $d_n := \text{card}\ (D_n)$. Pour tout $i \in F$, nous noterons $\mathcal{F}_i$ l'ensemble des bijections $f : F \to F$ telles que $f(i) = i$.

(a) Montrer que $D_n = S_n \setminus \bigcup_{i=1}^{n} \mathcal{F}_i$.

(b) Vérifier que

$$\begin{aligned} \text{card} \bigcup_{i=1}^{n} \mathcal{F}_i &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \text{card}\ (\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}) \\ &= \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! \end{aligned}$$

Indication : noter que $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des permutations telles que $f(i_1) = i_1, \ldots, f(i_k) = i_k$. Il est donc facile de les compter.

(c) Conclure que $d_n = n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

On verra en cours d'analyse (une autre année !) que $\lim_{n \to +\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \frac{1}{e}$. Donc $d_n \sim \frac{n!}{e}$.